REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

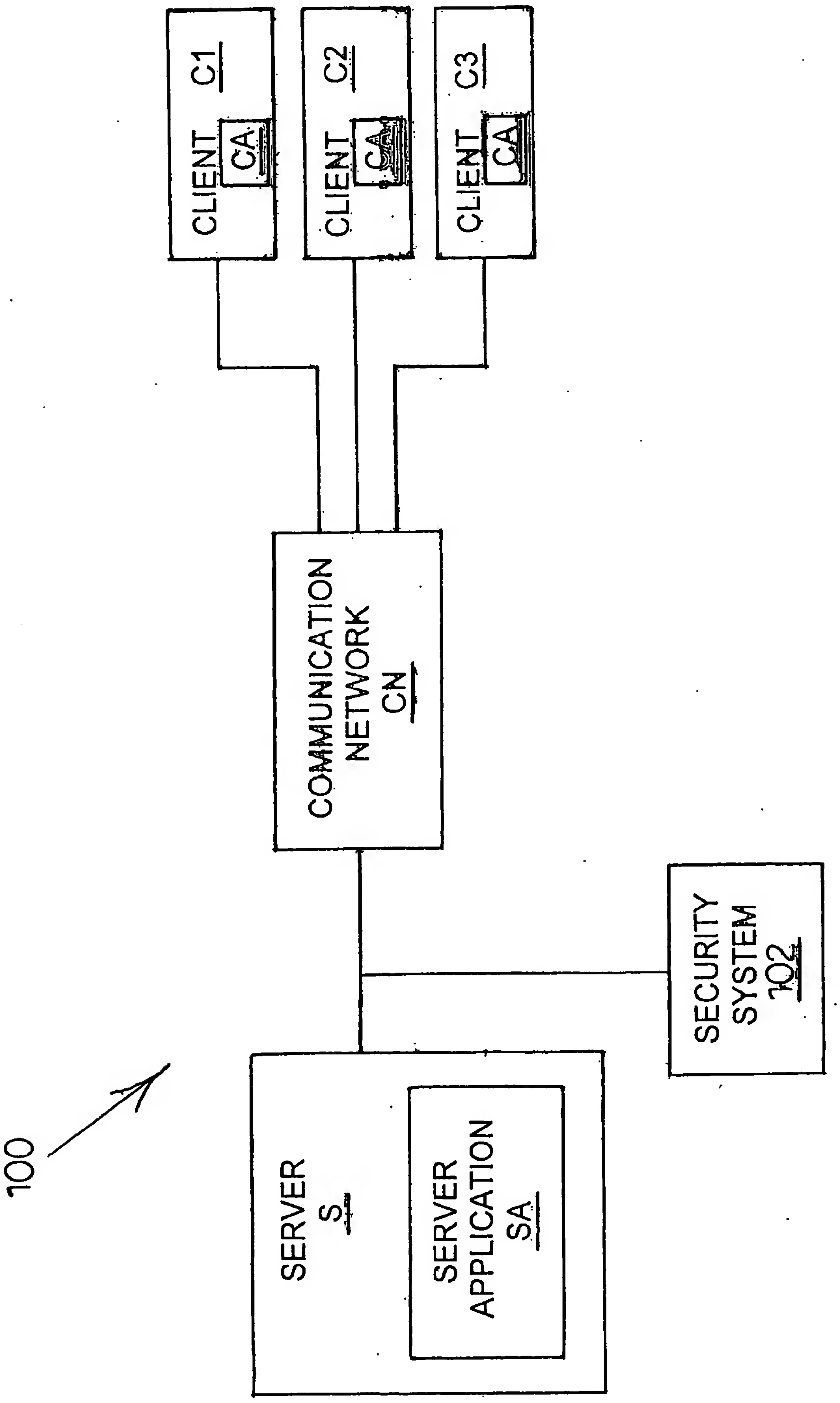


FiG 1A

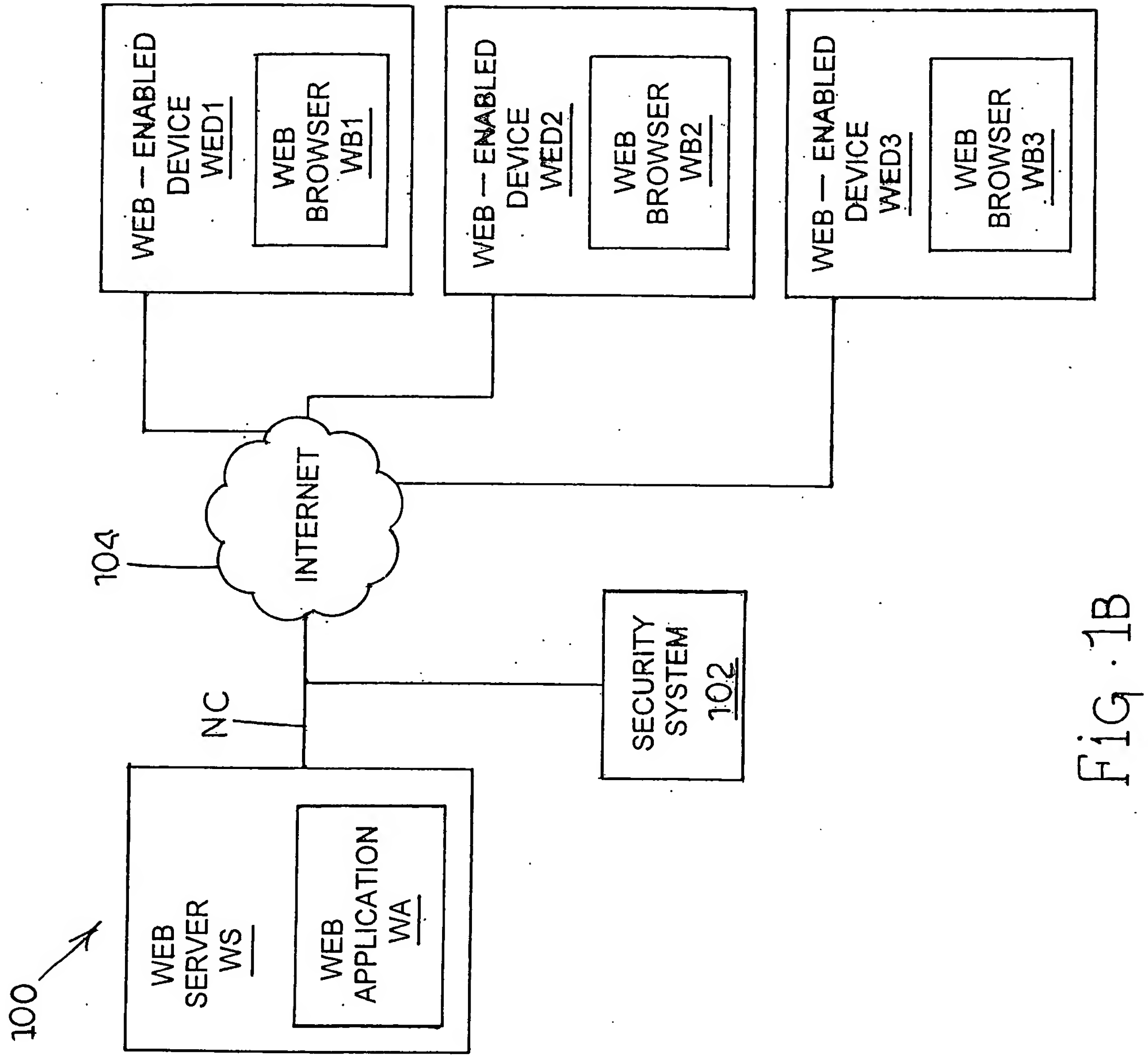

WEB — ENABLED DEVICE WED1
WEB BROWSER WB1
WEB — ENABLED DEVICE WED2
WEB BROWSER WB2
WEB — ENABLED DEVICE WED3
WEB BROWSER WB3
104
INTERNET
SECURITY SYSTEM 102
NC
100
WEB SERVER WS
WEB APPLICATION WA

FiG. 1B

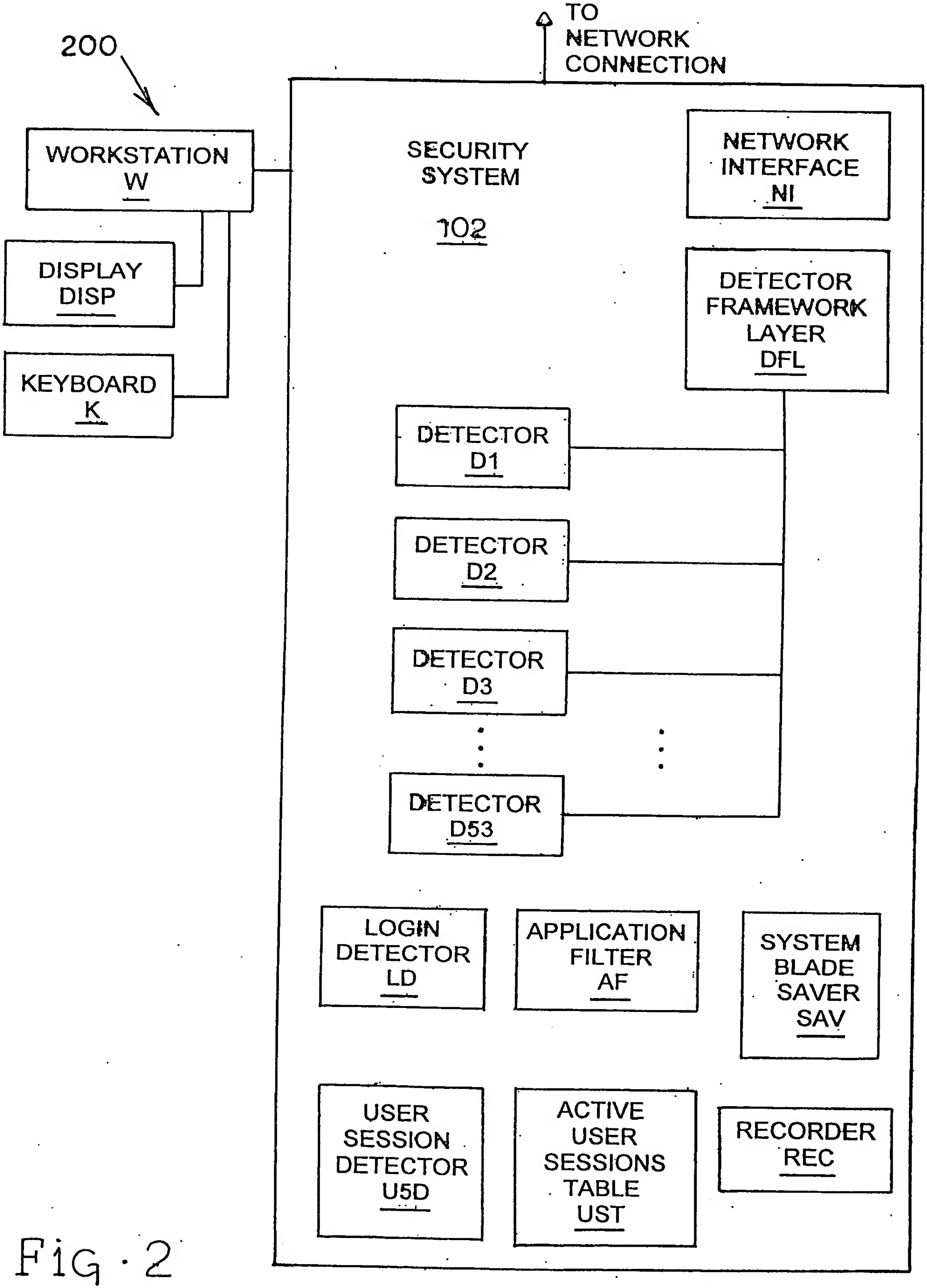

200
TO NETWORK CONNECTION
WORKSTATION W
DISPLAY DISP
KEYBOARD K
SECURITY SYSTEM
102
NETWORK INTERFACE NI
DETECTOR FRAMEWORK LAYER DFL
DETECTOR D1
DETECTOR D2
DETECTOR D3
DETECTOR D53
LOGIN DETECTOR LD
APPLICATION FILTER AF
SYSTEM BLADE SAVER SAV
USER SESSION DETECTOR U5D
ACTIVE USER SESSIONS TABLE UST
RECORDER REC

Fig. 2

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

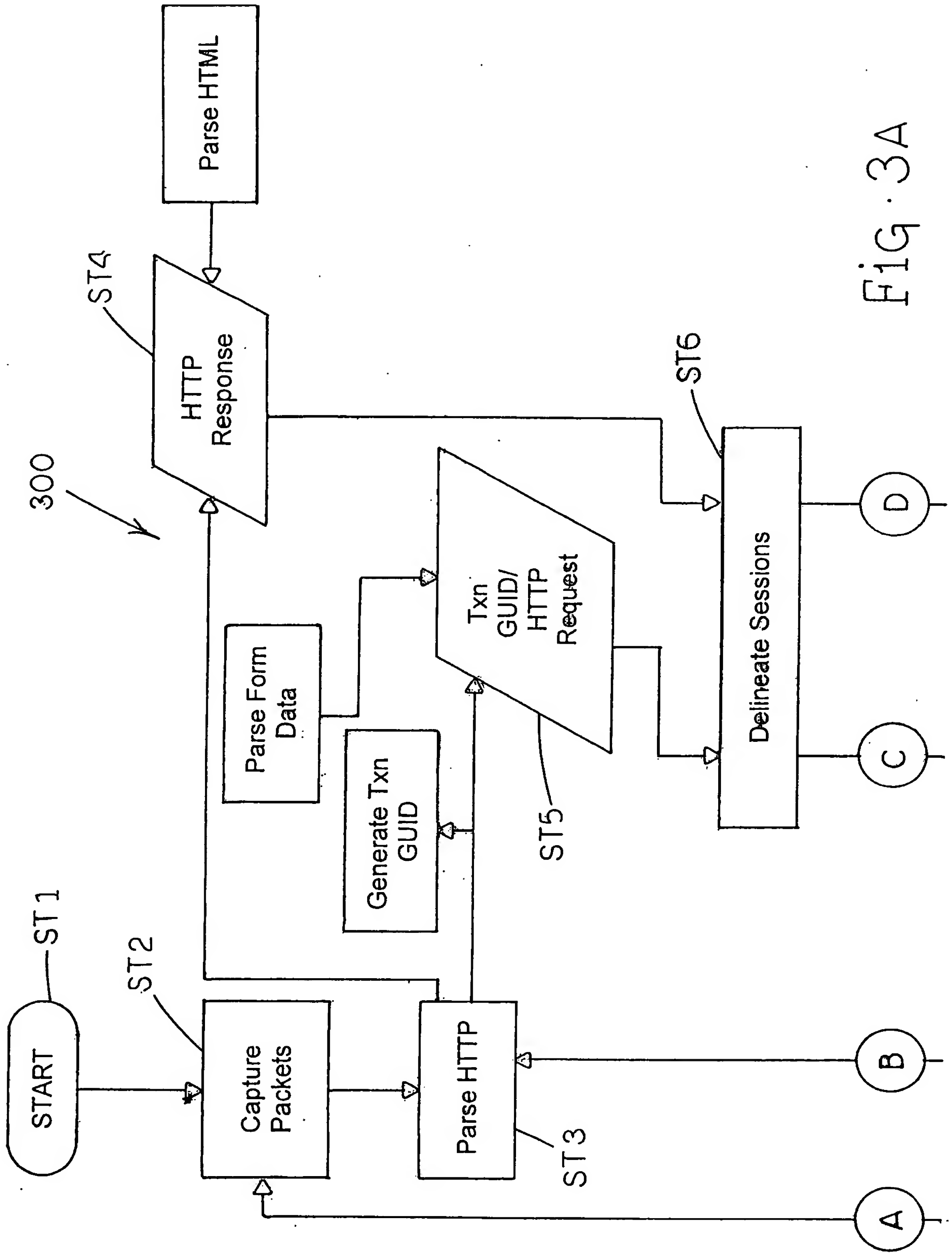


FIG. 3A

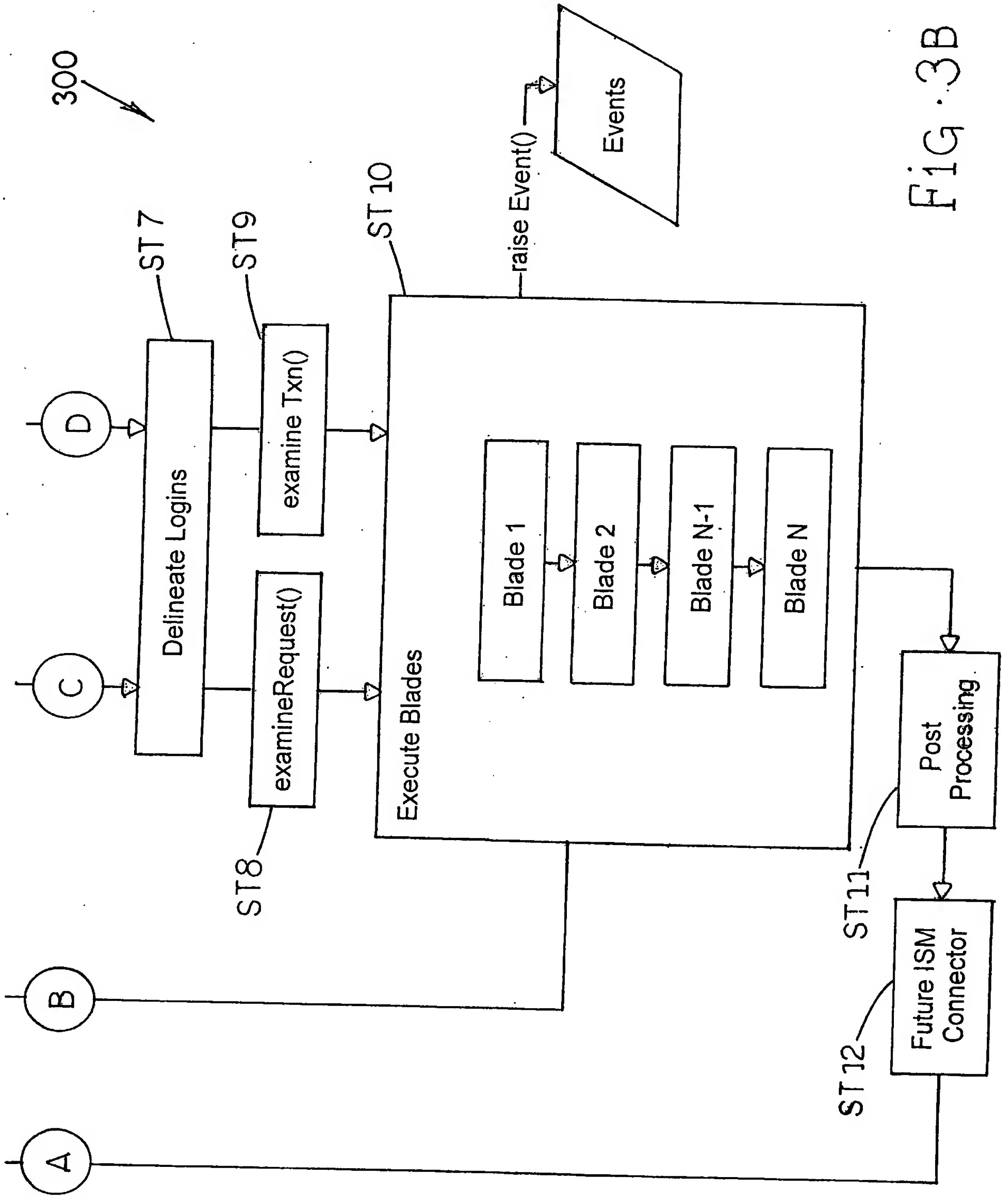
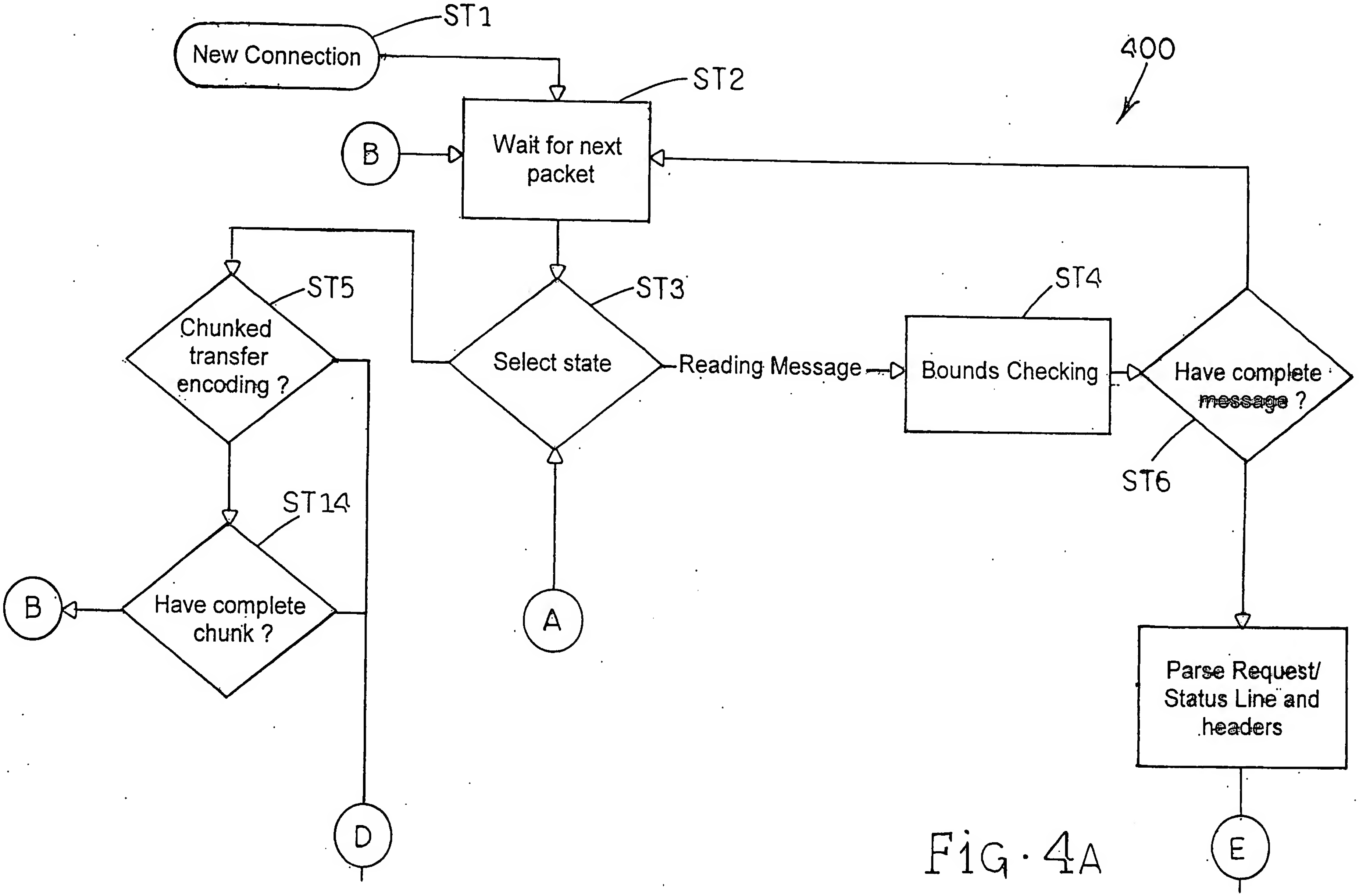

300
ST 7
ST9
ST 10
raise Event()
Events
D
C
Delineate Logins
examine Txn()
examineRequest()
ST8
Execute Blades
Blade 1
Blade 2
Blade N-1
Blade N
Post Processing
ST11
Future ISM Connector
ST 12
B
A

FiG.3B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6



FiG·4A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

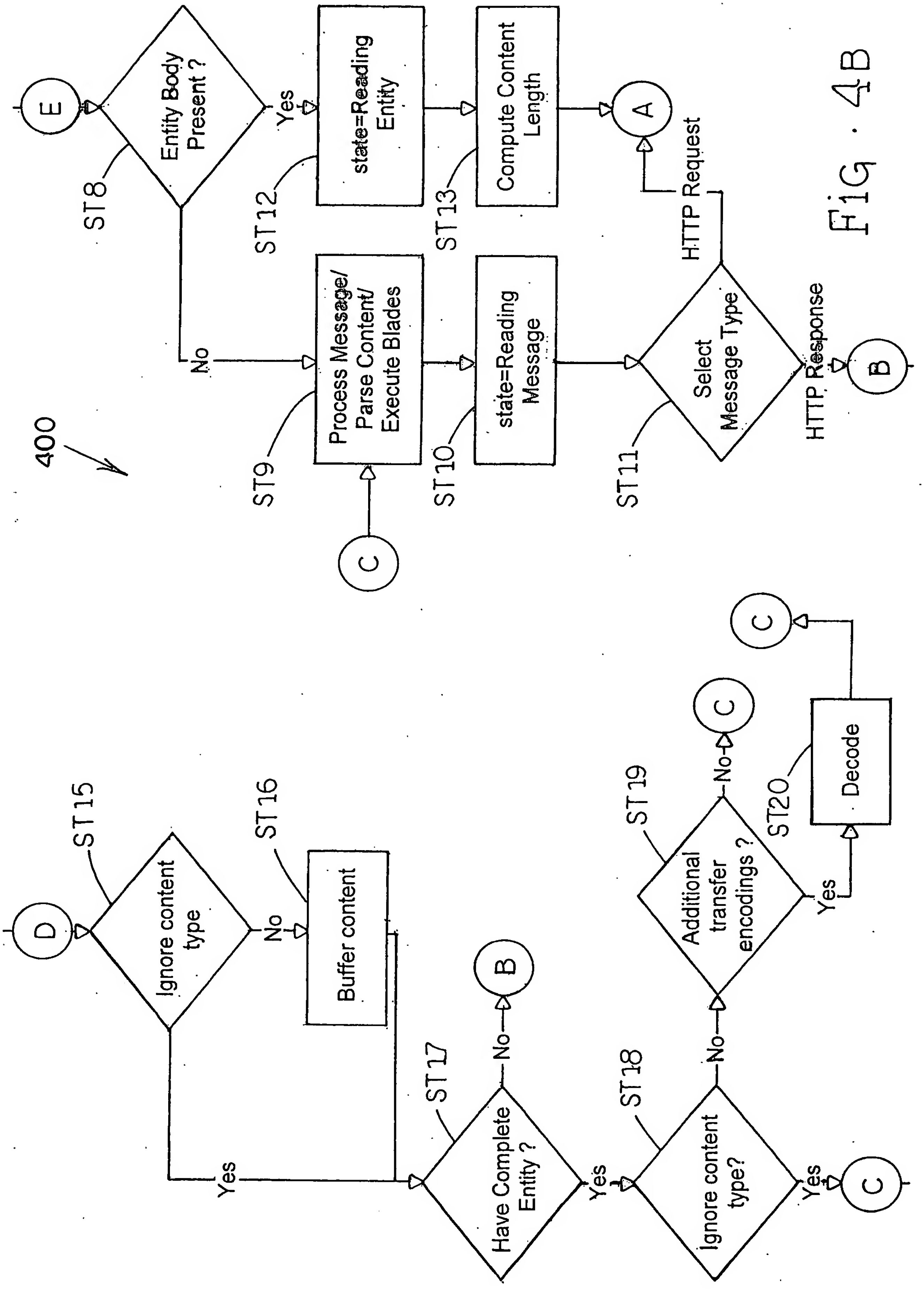
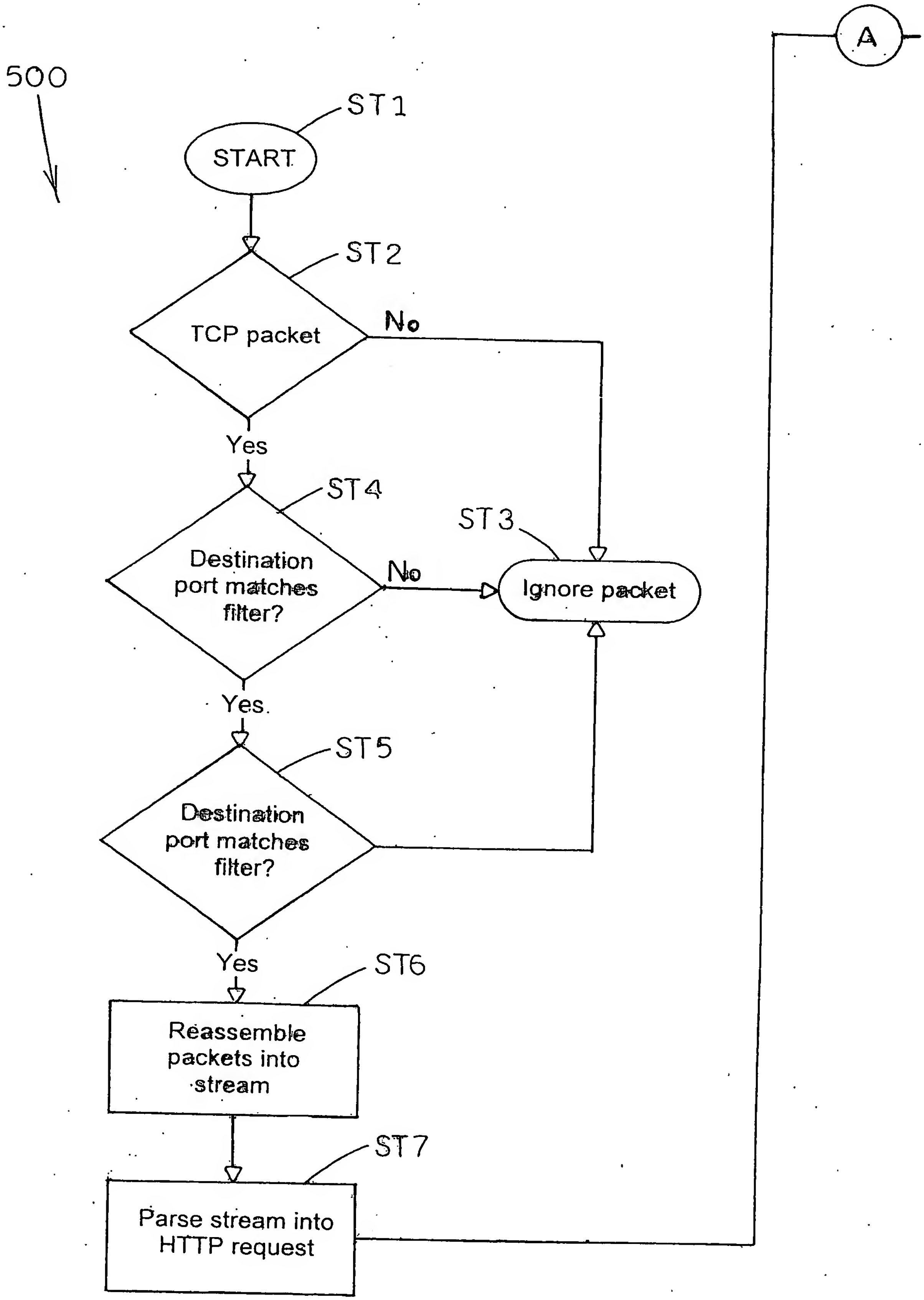


Fig. 4B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6



500
ST1
START
ST2
TCP packet
No
Yes
ST4
Destination port matches filter?
No
ST3
Ignore packet
Yes.
ST5
Destination port matches filter?
Yes
ST6
Reassemble packets into stream
ST7
Parse stream into HTTP request
A

FiG·5A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

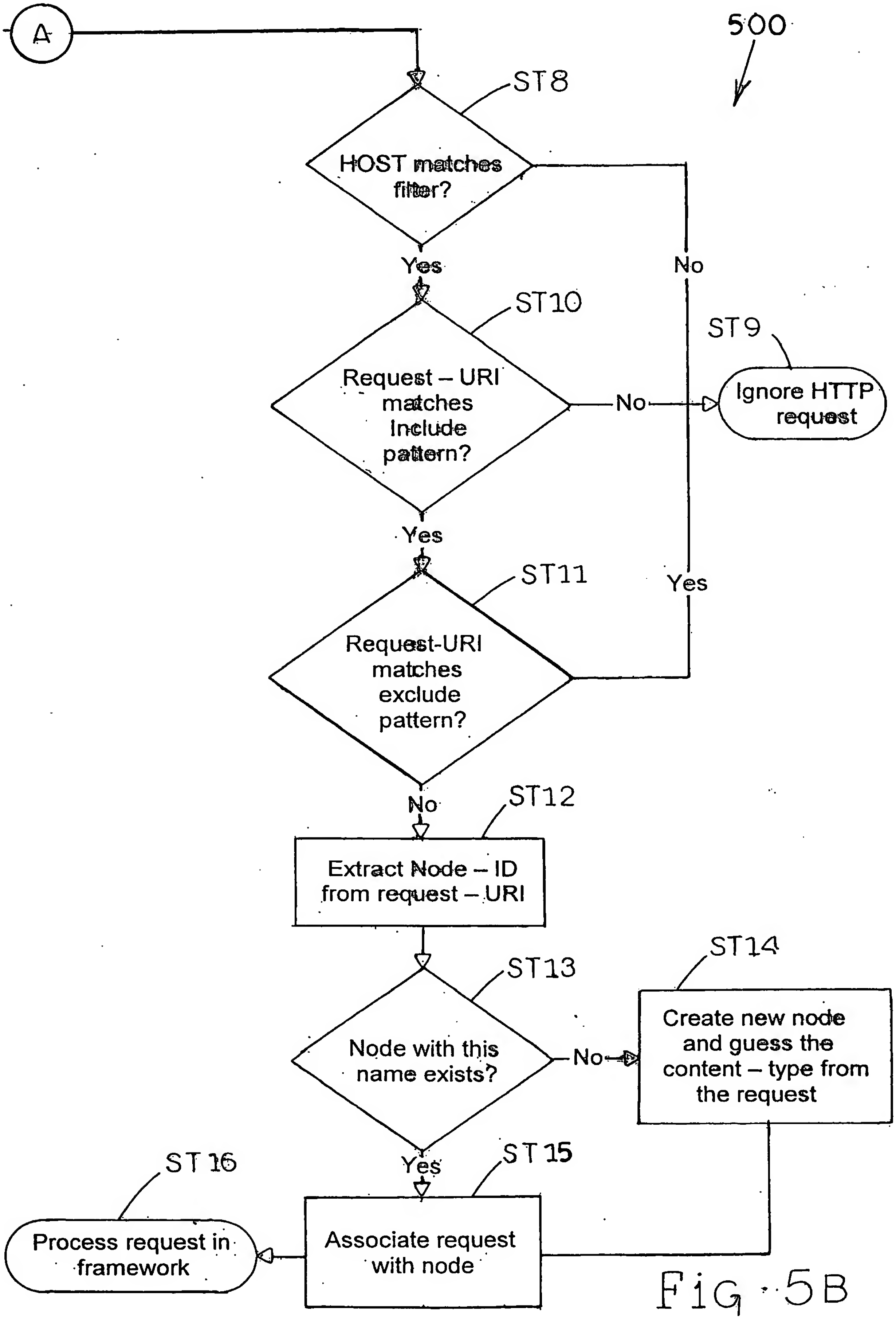

A
500
ST8
HOST matches filter?
Yes
No
ST10
Request – URI matches Include pattern?
No
ST9
Ignore HTTP request
Yes
ST11
Yes
Request-URI matches exclude pattern?
No
ST12
Extract Node – ID from request – URI
ST13
Node with this name exists?
No
ST14
Create new node and guess the content – type from the request
Yes
ST 15
ST 16
Process request in framework
Associate request with node

FiG 5B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

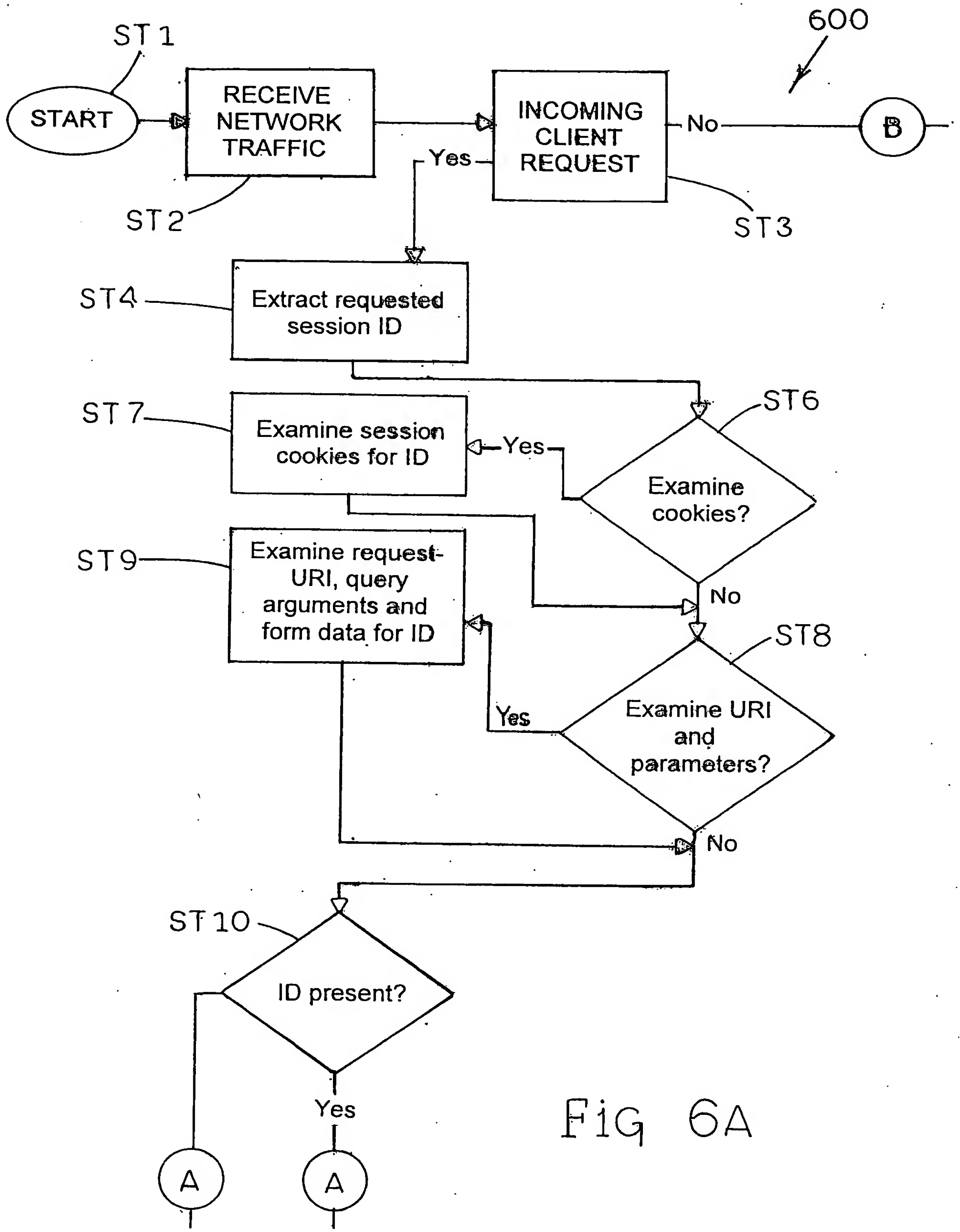

600
ST1
START
RECEIVE NETWORK TRAFFIC
ST2
INCOMING CLIENT REQUEST
ST3
No
B
Yes
ST4
Extract requested session ID
ST6
Examine cookies?
Yes
ST 7
Examine session cookies for ID
No
ST8
ST9
Examine request-URI, query arguments and form data for ID
Examine URI and parameters?
Yes
No
ST10
ID present?
Yes
A
A

Fig 6A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

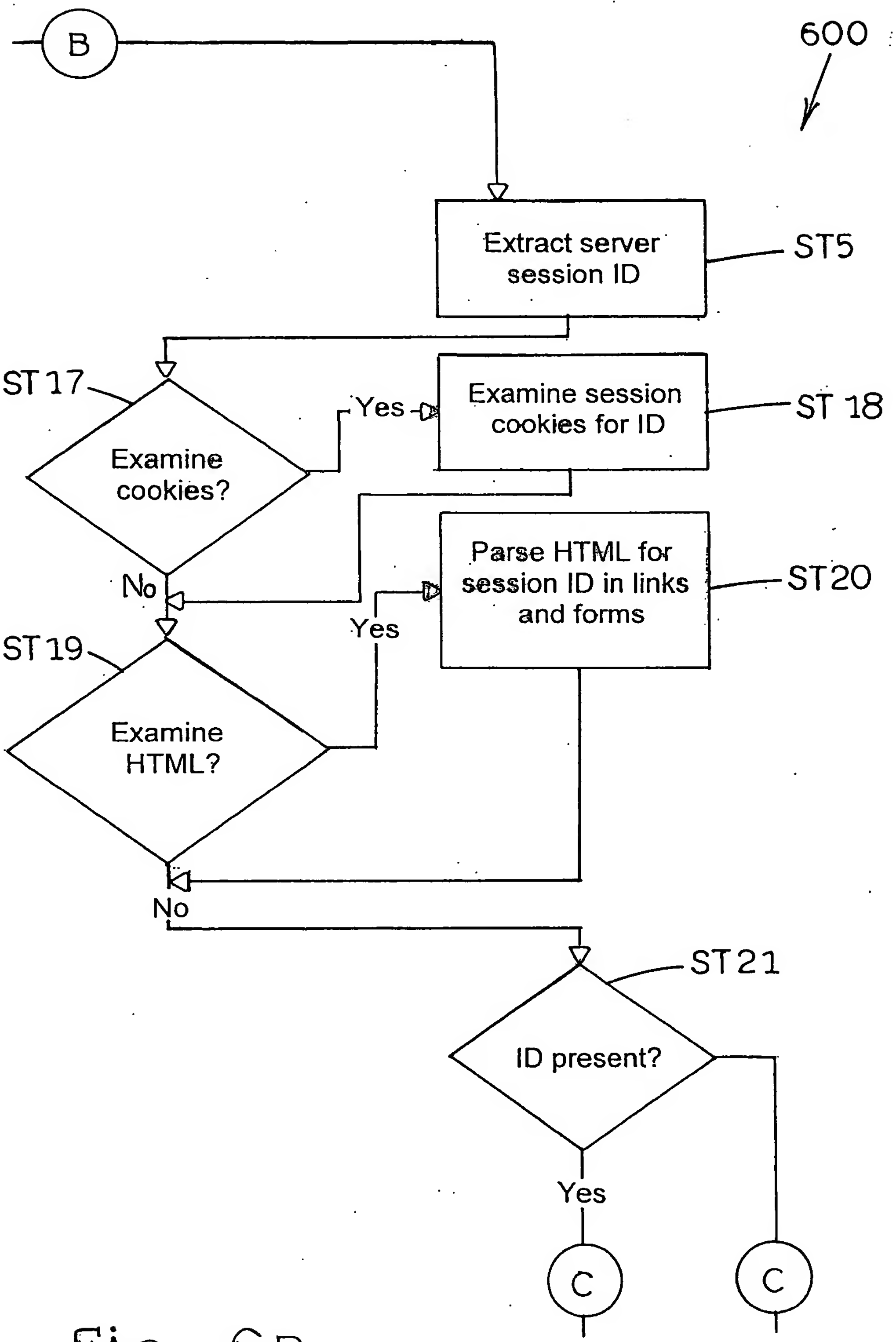

B
600
Extract server session ID
ST5
ST 17
Examine cookies?
Yes
Examine session cookies for ID
ST 18
No
Parse HTML for session ID in links and forms
ST20
ST 19
Yes
Examine HTML?
No
ST21
ID present?
Yes
C
C

FIG. 6B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER
PROGRAM PRODUCTS FOR MONITORING A
SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

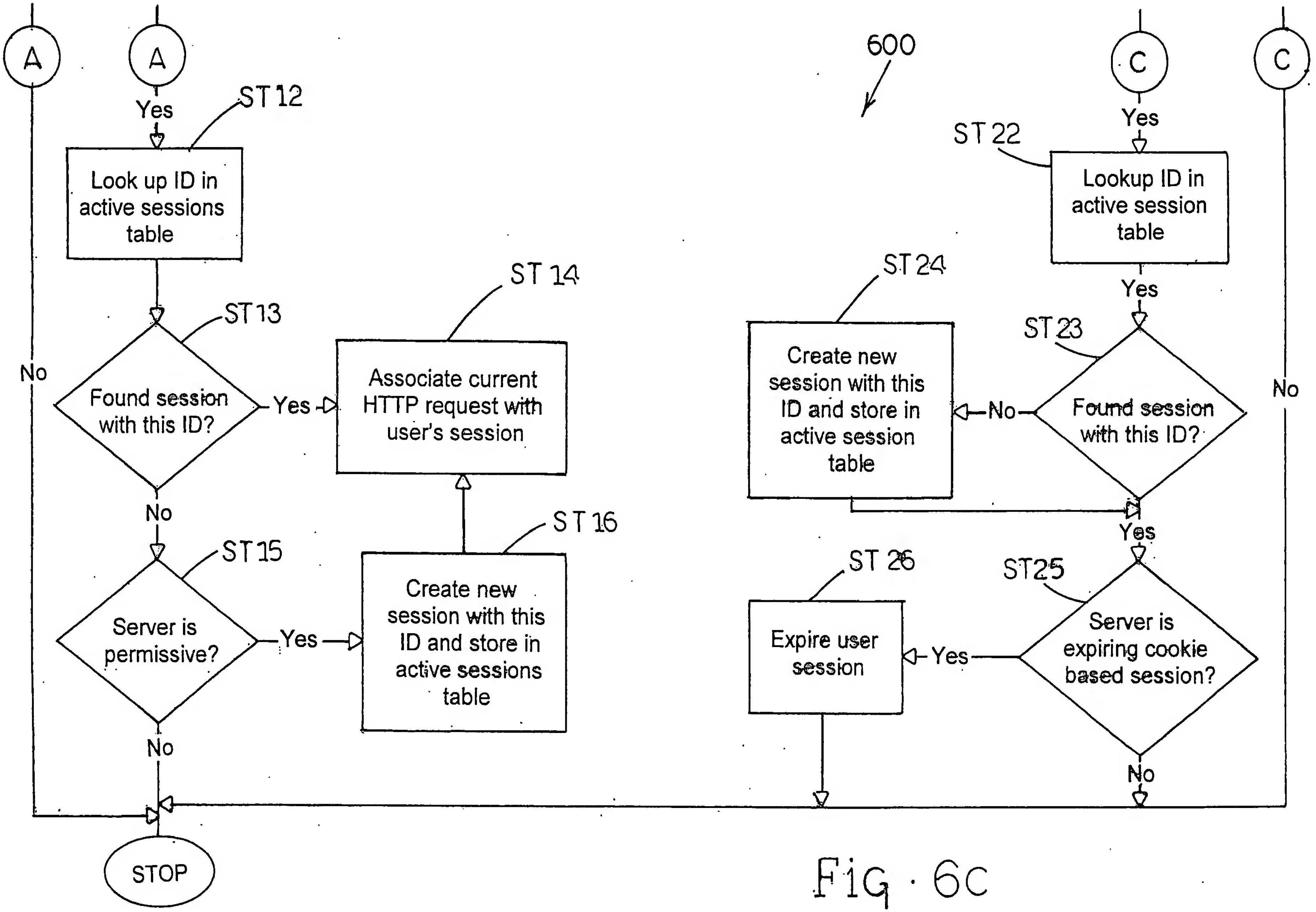

A
A
No
Yes
ST12
Look up ID in active sessions table
ST13
Found session with this ID?
Yes
No
ST14
Associate current HTTP request with user's session
ST15
Server is permissive?
Yes
No
ST 16
Create new session with this ID and store in active sessions table
STOP
600
C
C
Yes
ST 22
Lookup ID in active session table
Yes
ST 23
Found session with this ID?
No
ST 24
Create new session with this ID and store in active session table
Yes
ST25
Server is expiring cookie based session?
Yes
No
ST 26
Expire user session
No

Fig. 6C

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

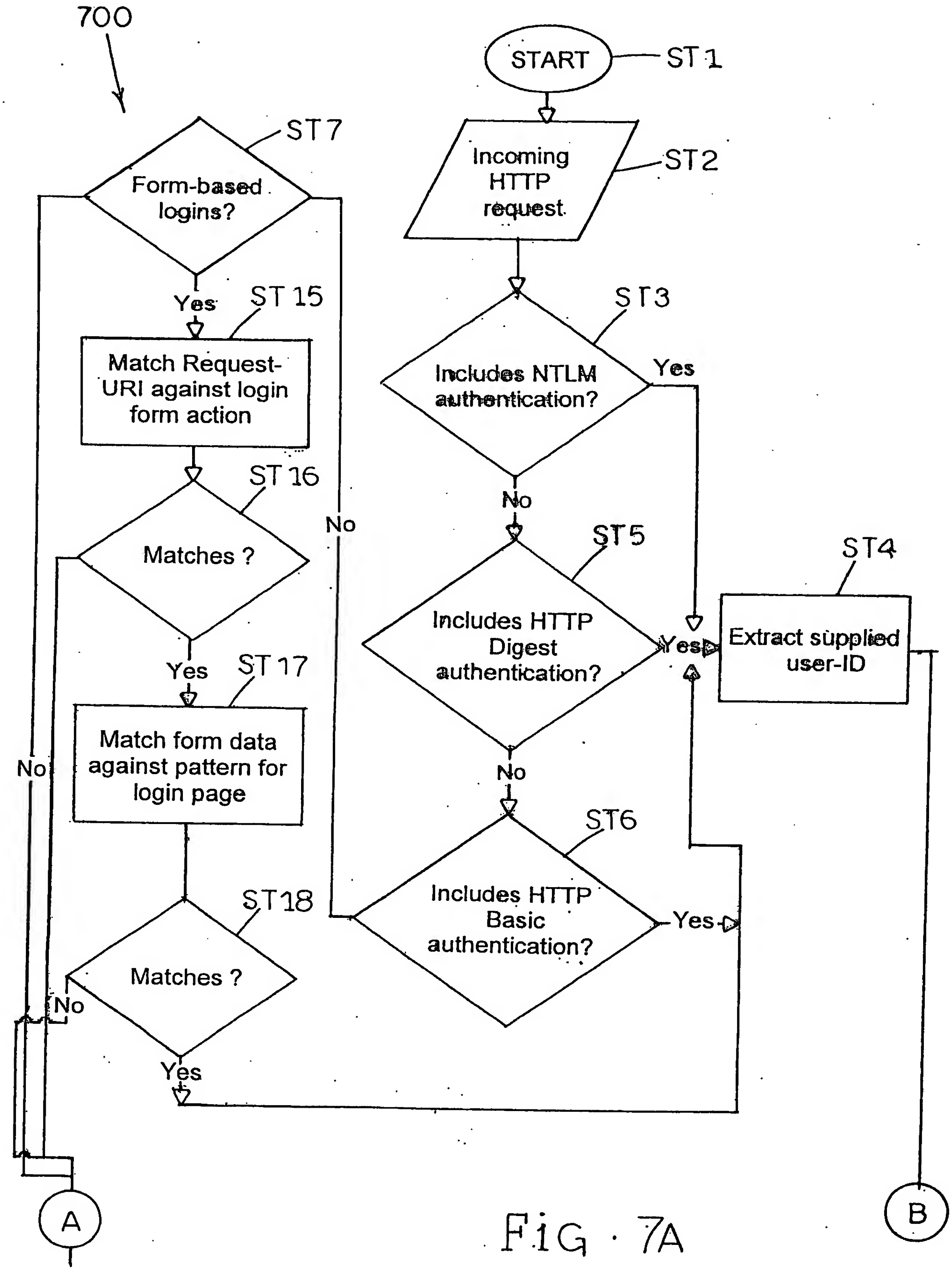

700
START
ST1
Incoming HTTP request
ST2
ST3
Includes NTLM authentication?
Yes
No
ST5
Includes HTTP Digest authentication?
Yes
No
ST6
Includes HTTP Basic authentication?
Yes
ST4
Extract supplied user-ID
ST7
Form-based logins?
Yes
No
ST15
Match Request-URI against login form action
ST16
Matches ?
Yes
No
ST17
Match form data against pattern for login page
ST18
Matches ?
No
Yes
A
B

FiG. 7A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER
PROGRAM PRODUCTS FOR MONITORING A
SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

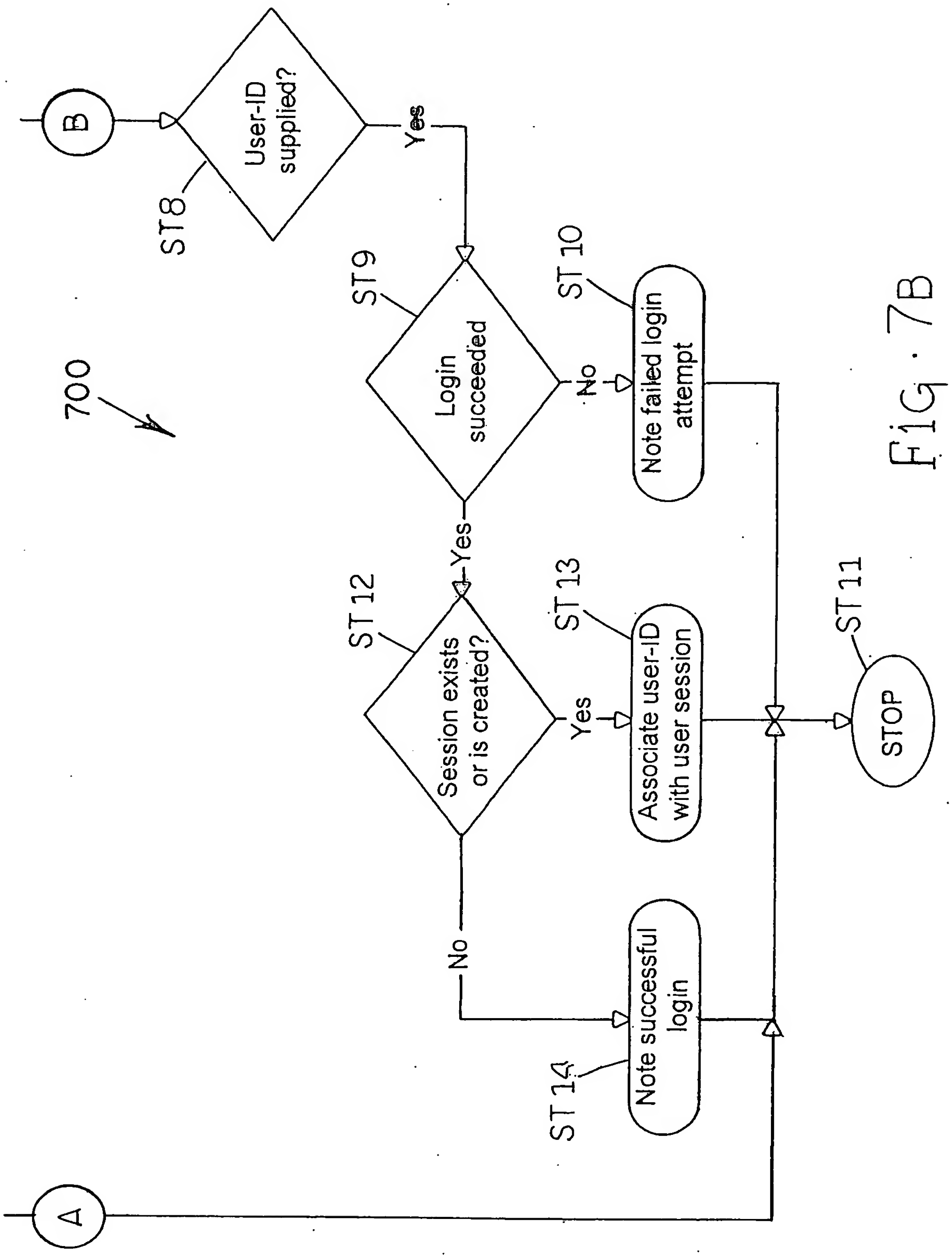


FiG. 7B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER
PROGRAM PRODUCTS FOR MONITORING A
SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

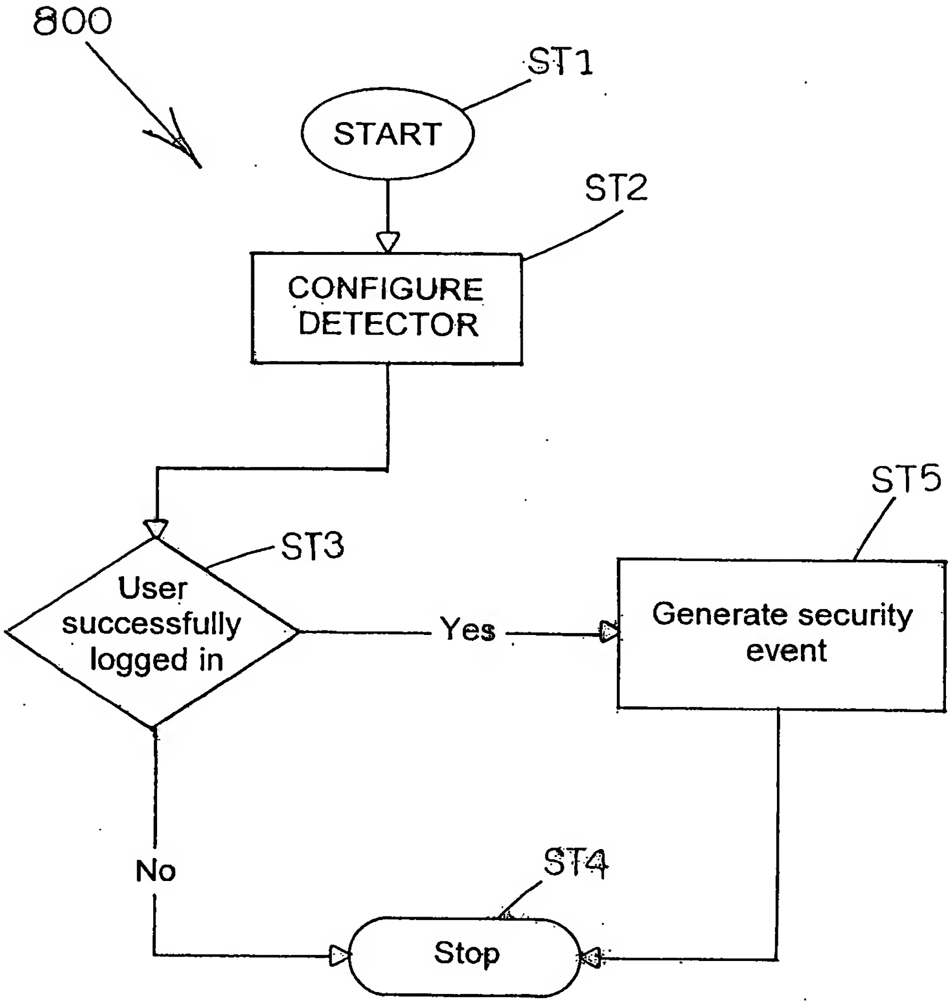


FiG. 8

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

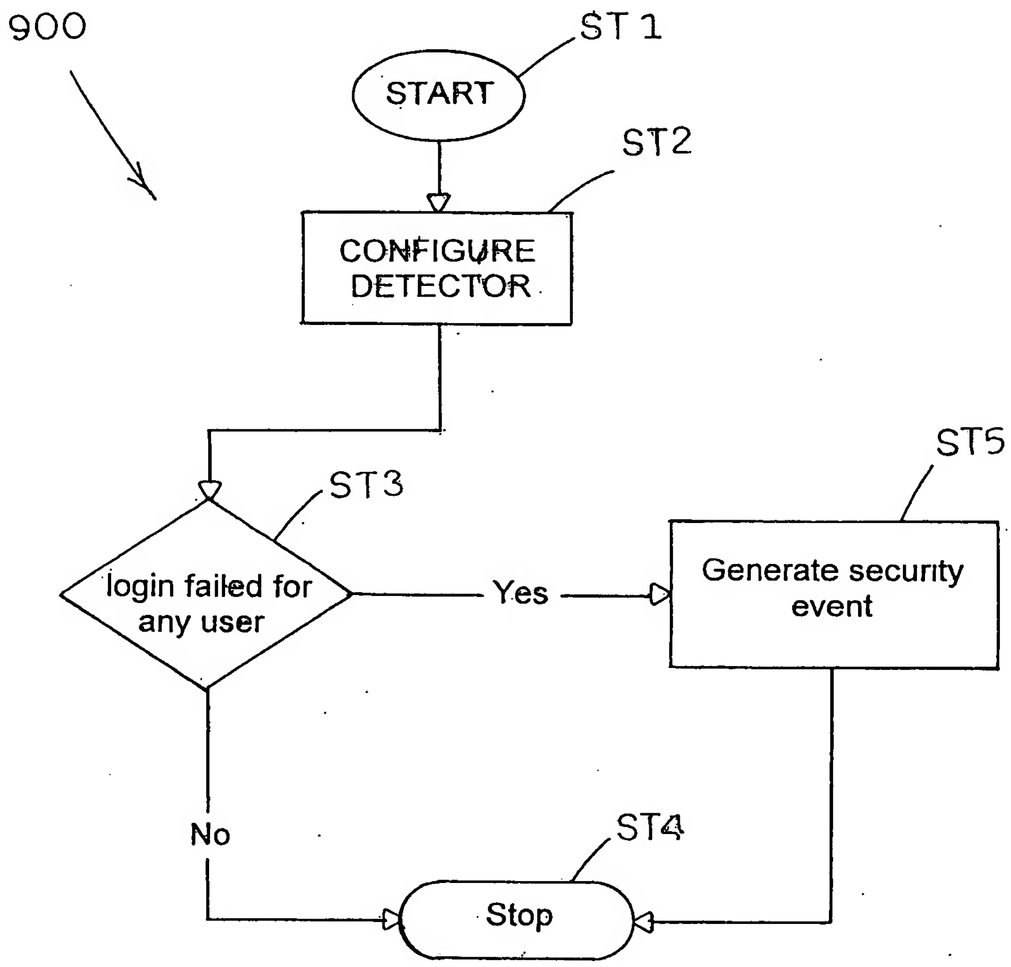


FiG · 9

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

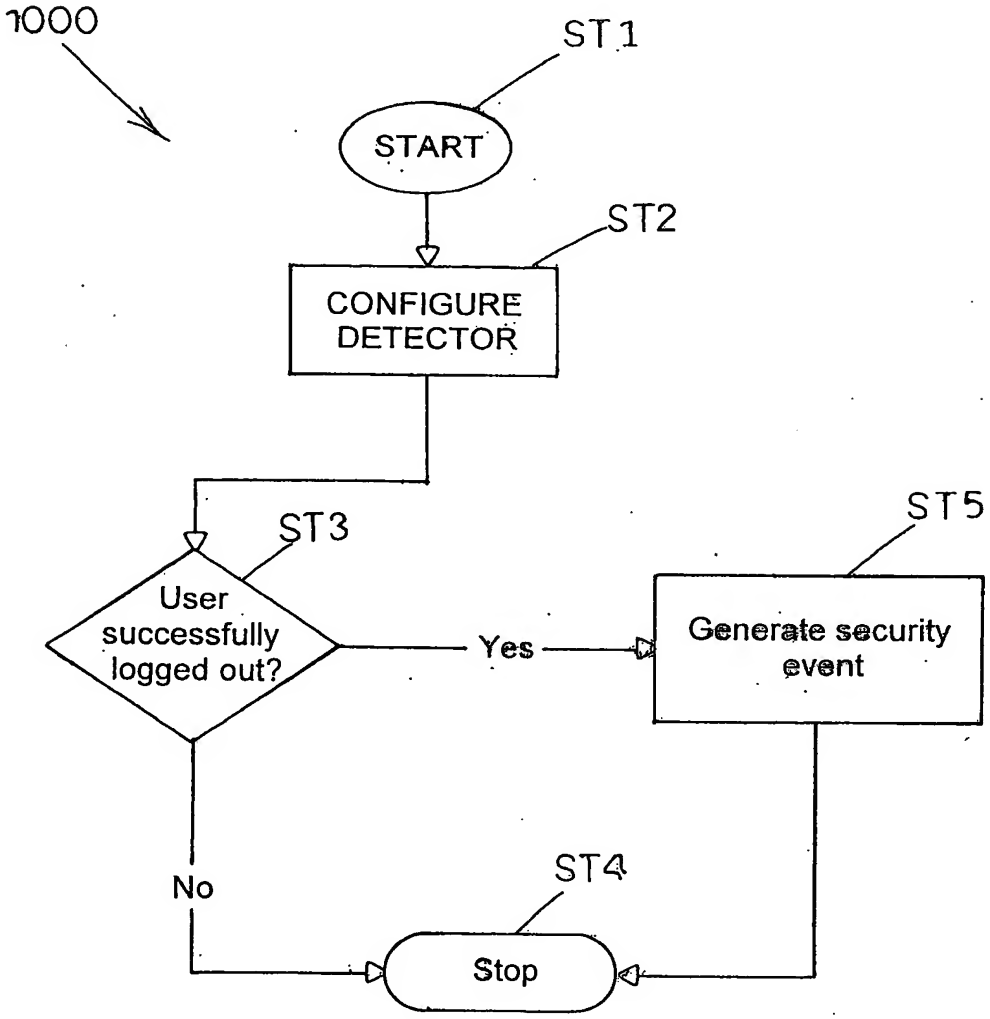


Fig. 10

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER
PROGRAM PRODUCTS FOR MONITORING A
SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

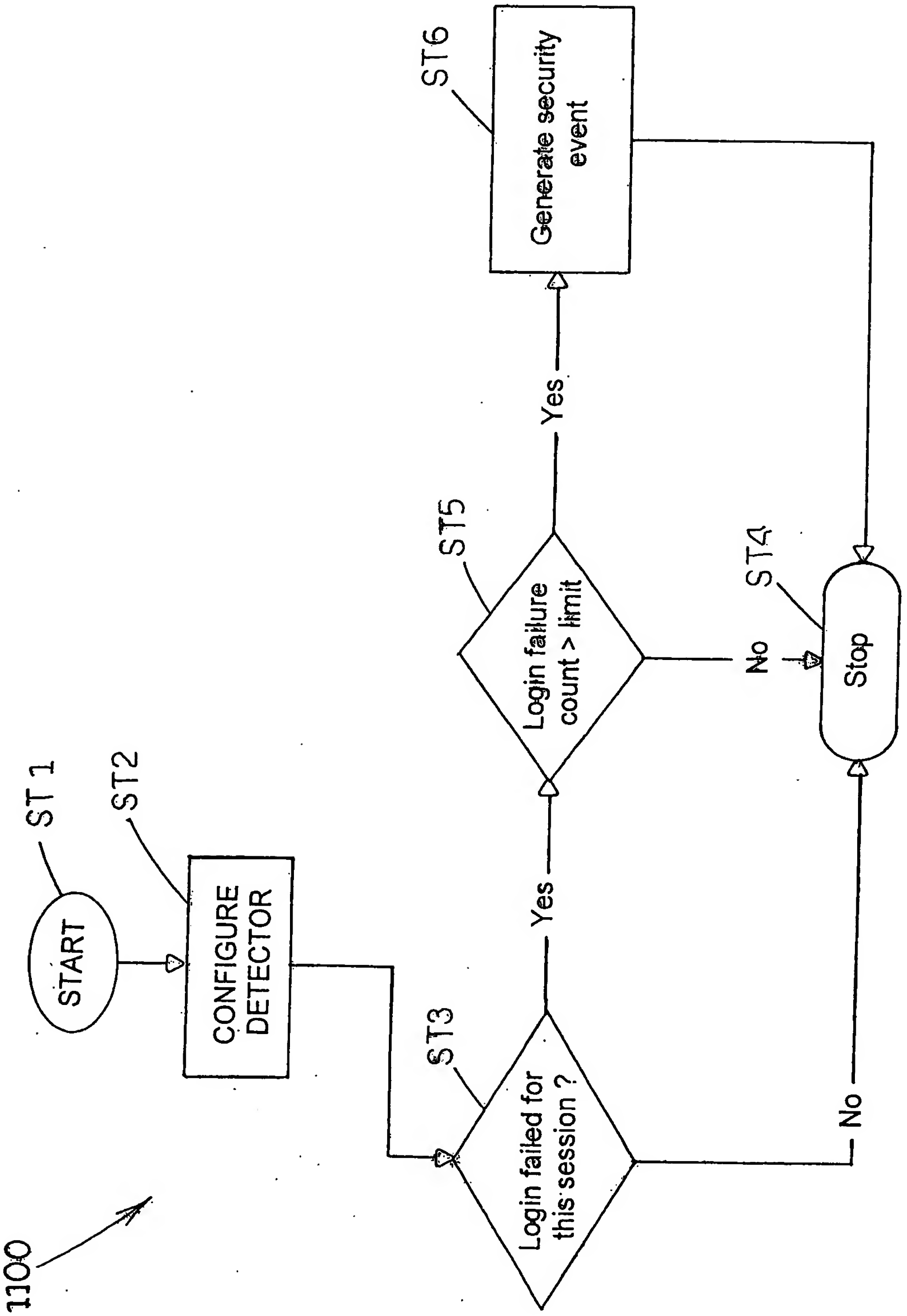


FIG. 11

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

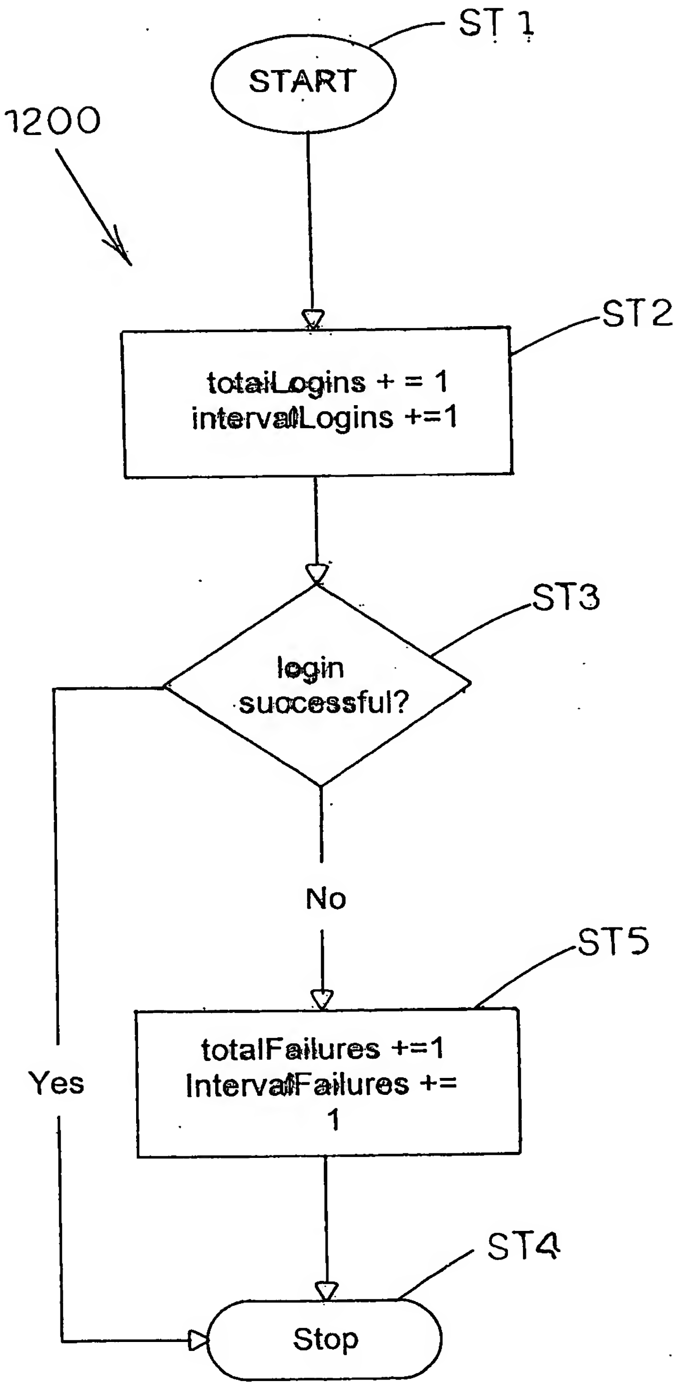


Fig. 12A

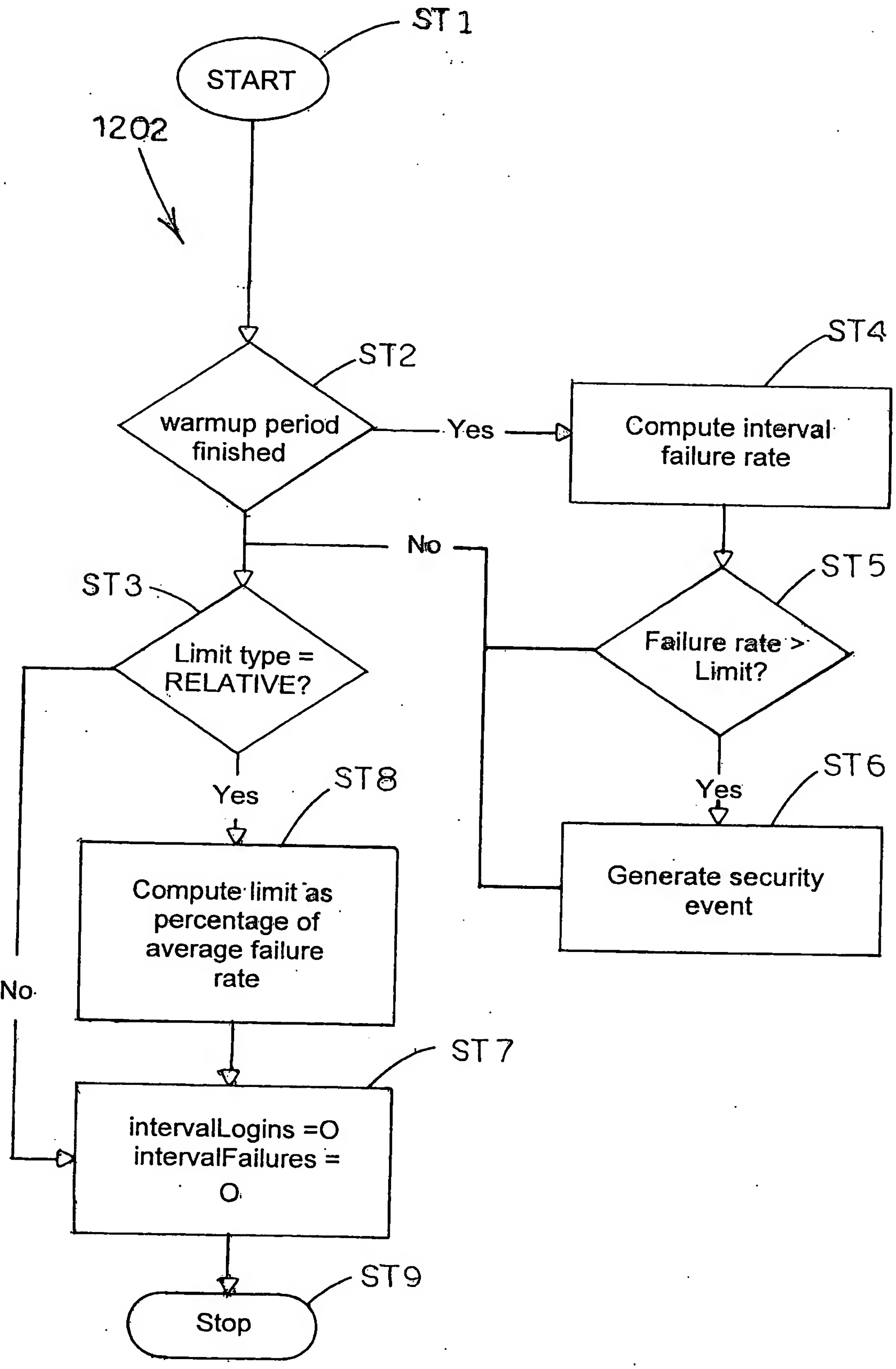

ST1
START
1202
ST2
warmup period finished
Yes
No
ST4
Compute interval failure rate
ST5
Failure rate > Limit?
Yes
ST6
Generate security event
ST3
Limit type = RELATIVE?
Yes
No
ST8
Compute limit as percentage of average failure rate
ST7
intervalLogins =O
intervalFailures = O
ST9
Stop

Fig ·12B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER
PROGRAM PRODUCTS FOR MONITORING A
SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

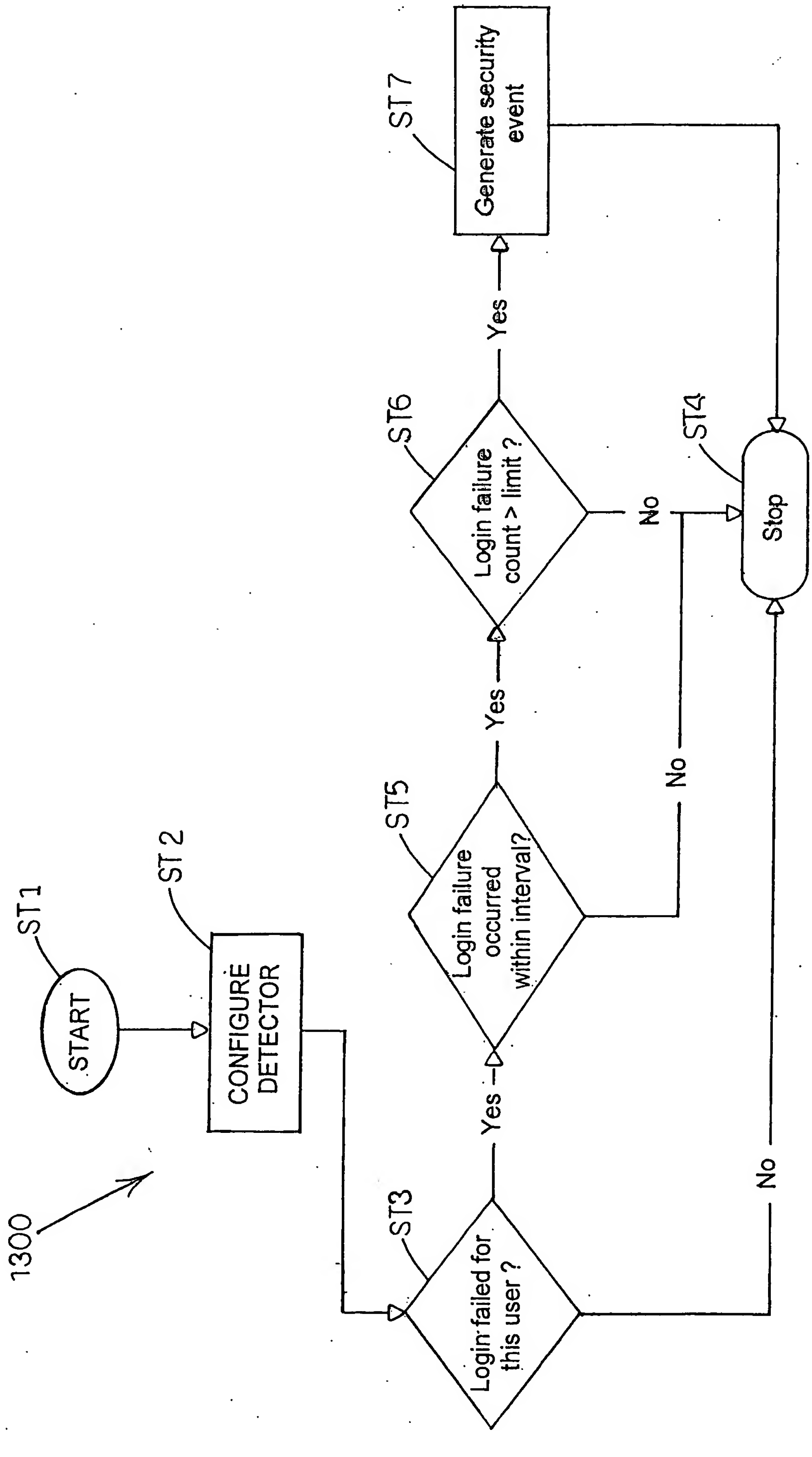

1300
ST1
START
ST 2
CONFIGURE DETECTOR
ST3
Login failed for this user ?
Yes
No
ST5
Login failure occurred within interval?
Yes
No
ST6
Login failure count > limit ?
Yes
No
ST 7
Generate security event
ST4
Stop

FIG. 13

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

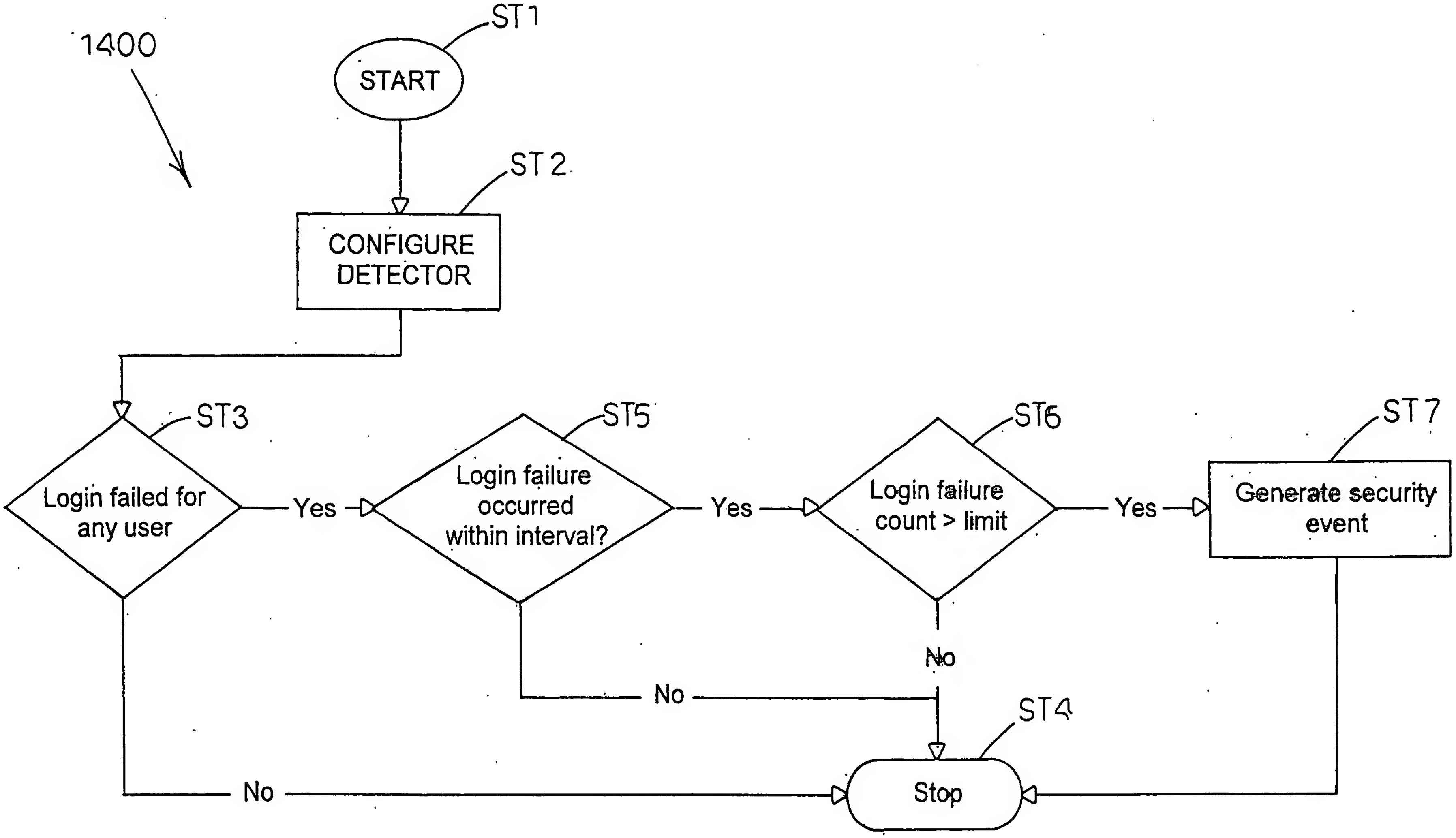

1400
ST1
START
ST 2
CONFIGURE DETECTOR
ST3
Login failed for any user
Yes
ST5
Login failure occurred within interval?
Yes
ST6
Login failure count > limit
Yes
ST7
Generate security event
No
No
ST4
Stop
No

Fig. 14

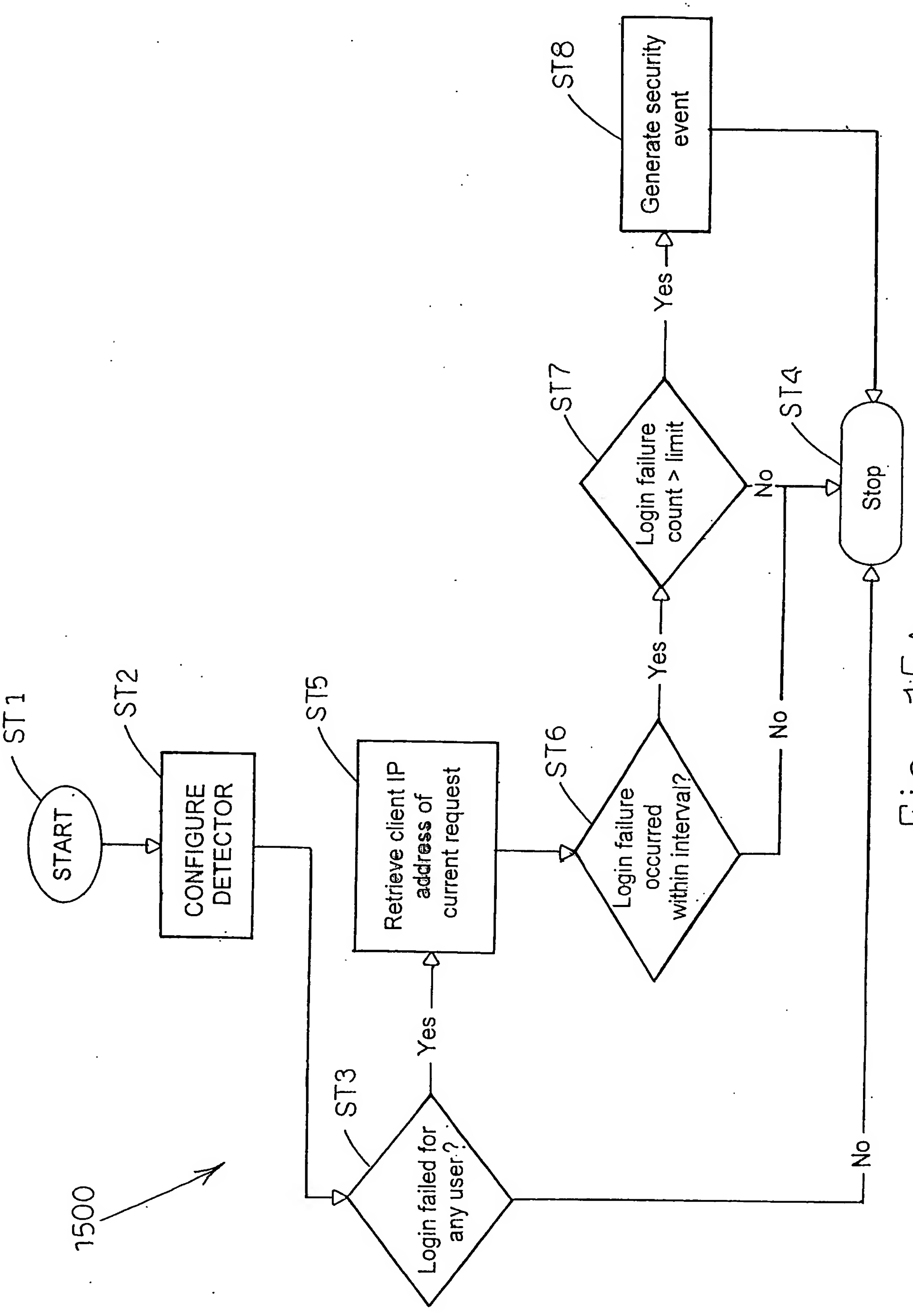

1500
ST1
START
ST2
CONFIGURE DETECTOR
ST3
Login failed for any user?
Yes
No
ST5
Retrieve client IP address of current request
ST6
Login failure occurred within interval?
Yes
No
ST7
Login failure count > limit
Yes
No
ST8
Generate security event
ST4
Stop

FIG. 15A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

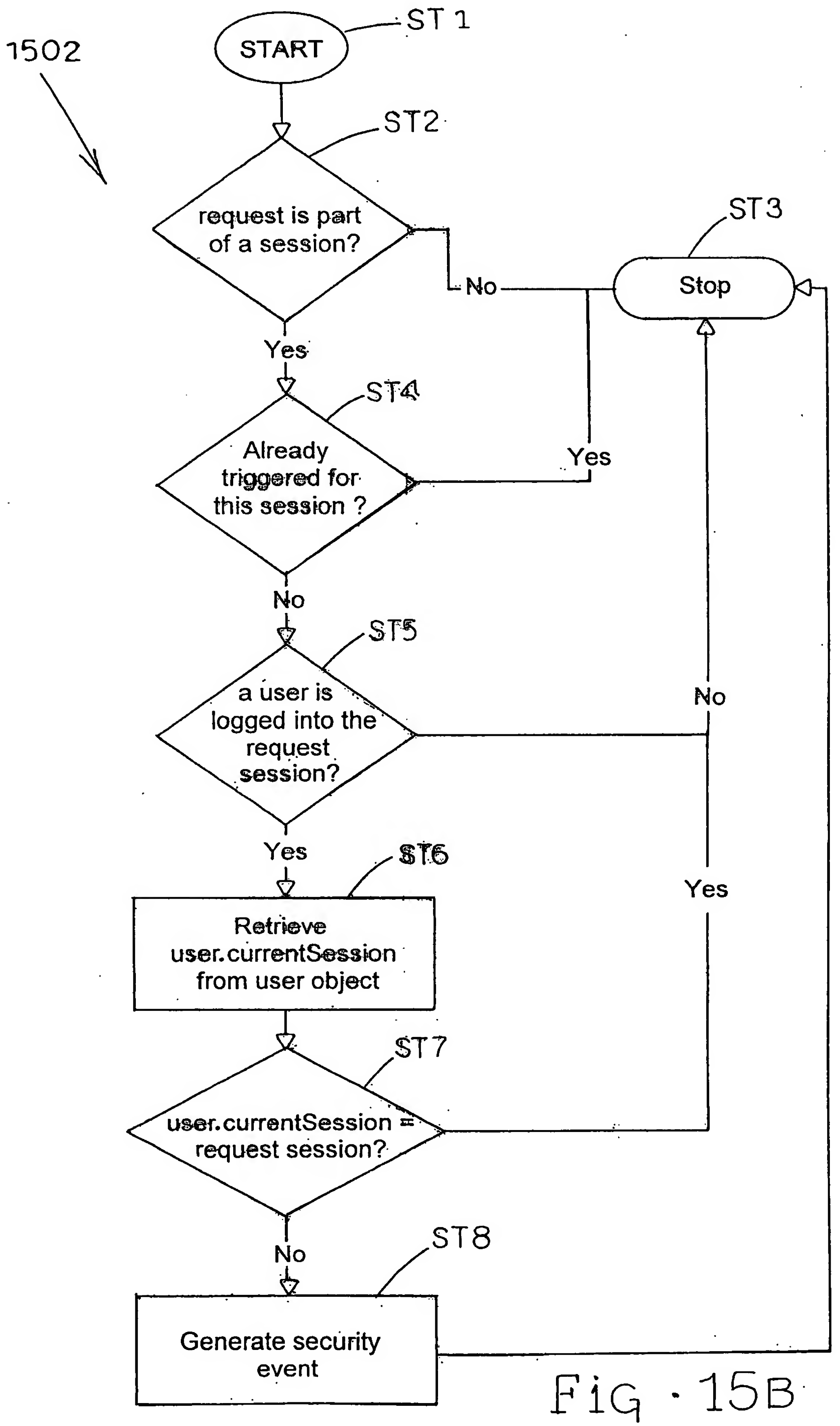

1502
ST 1
START
ST2
request is part of a session?
No
ST3
Stop
Yes
ST4
Already triggered for this session ?
Yes
No
ST5
a user is logged into the request session?
No
Yes
ST6
Retrieve user.currentSession from user object
Yes
ST7
user.currentSession = request session?
No
ST8
Generate security event

Fig. 15B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

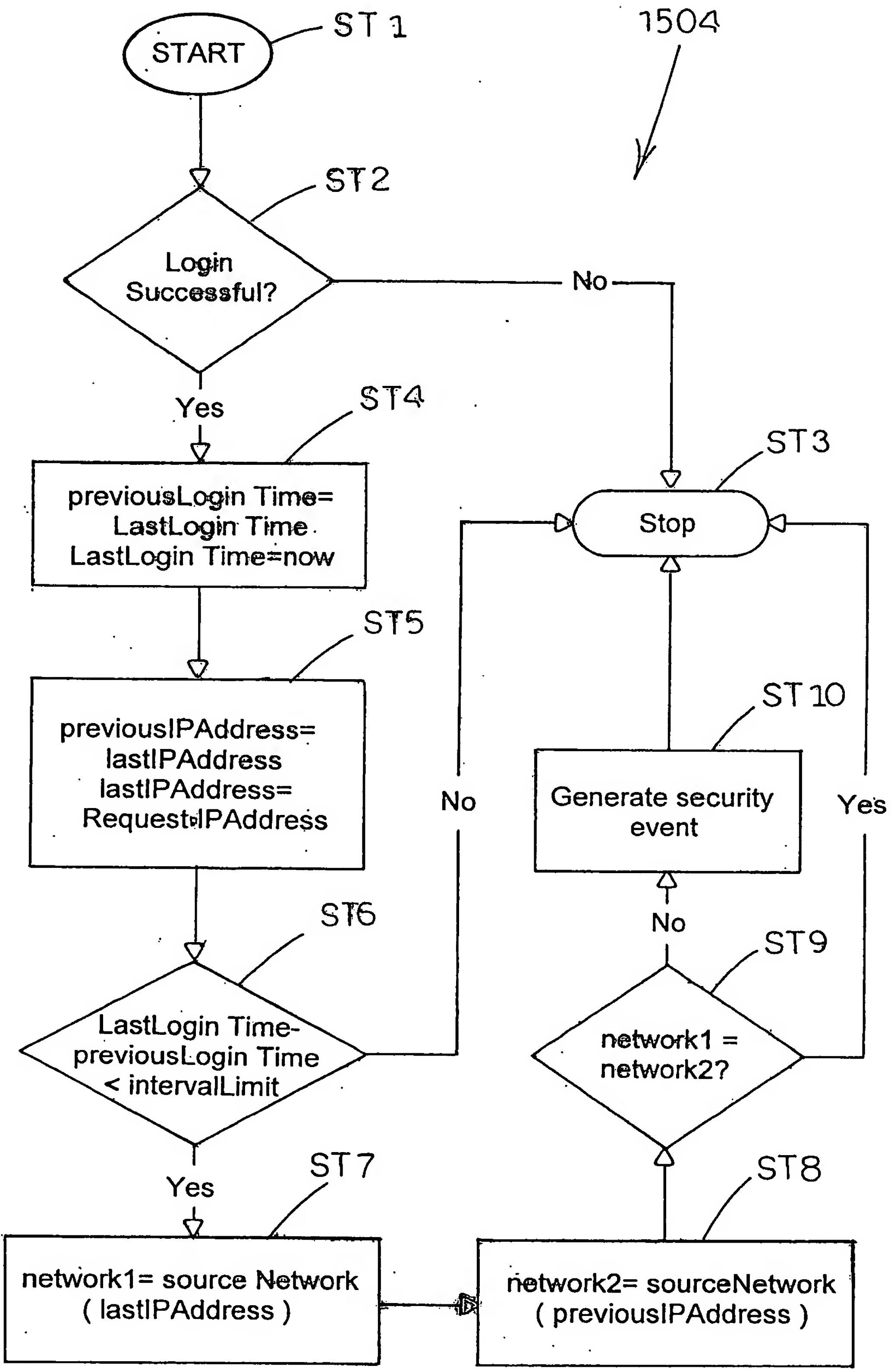

ST 1
START
1504
ST2
Login Successful?
No
Yes
ST4
previousLogin Time= LastLogin Time LastLogin Time=now
ST3
Stop
ST5
previousIPAddress= lastIPAddress lastIPAddress= RequestIPAddress
ST 10
Generate security event
No
Yes
No
ST6
LastLogin Time-previousLogin Time < intervalLimit
ST9
network1 = network2?
Yes
ST7
ST8
network1= source Network (lastIPAddress)
network2= sourceNetwork (previousIPAddress)

Fig. 15c

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

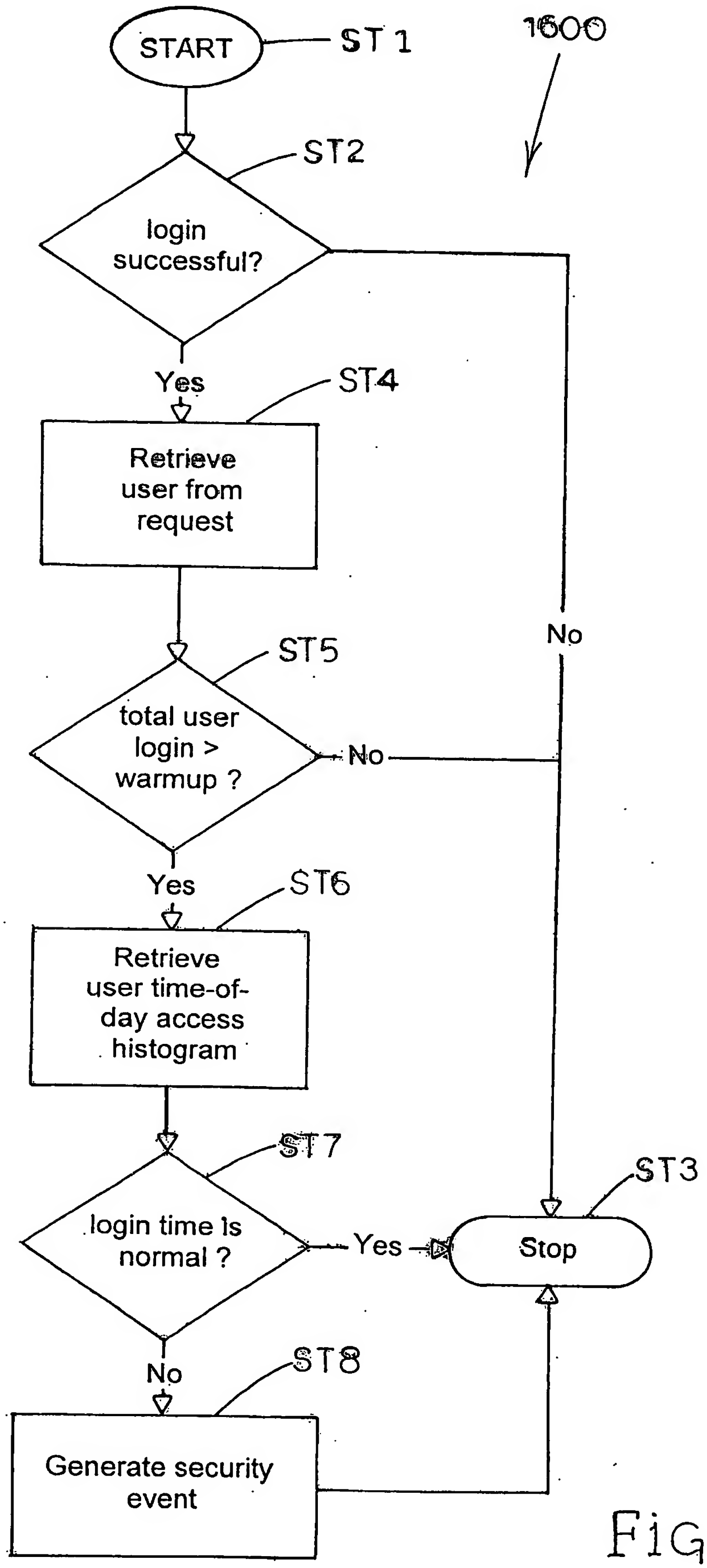


FiG · 16A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

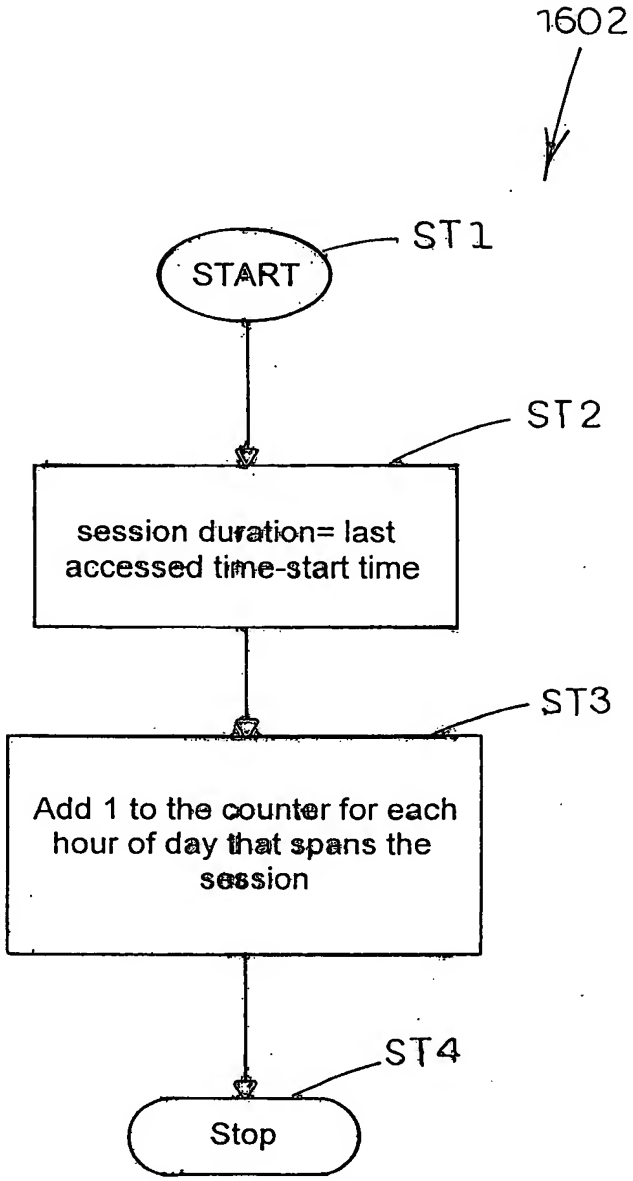
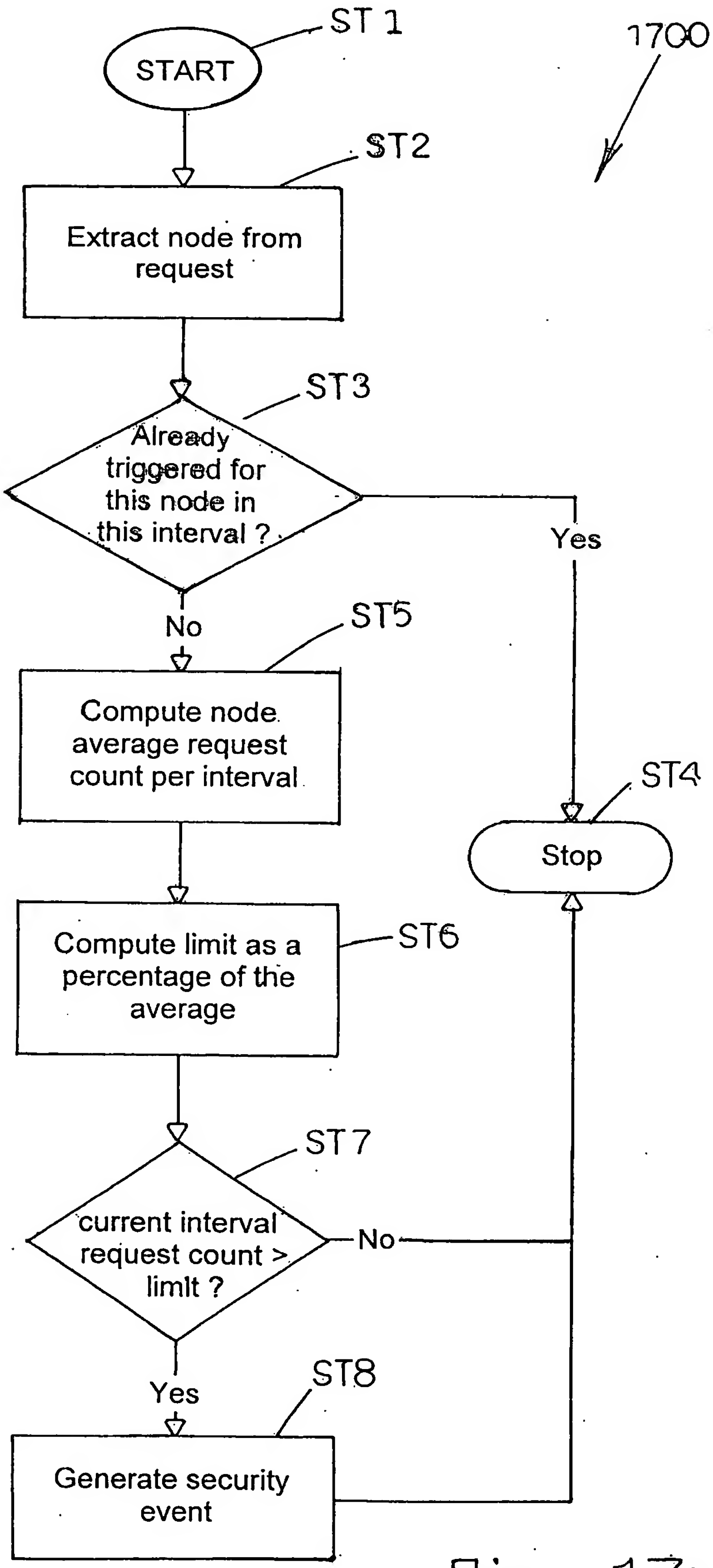

1602
START
ST1
ST2
session duration= last accessed time-start time
ST3
Add 1 to the counter for each hour of day that spans the session
ST4
Stop

FIG. 16B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6



ST 1
START
1700
ST2
Extract node from request
ST3
Already triggered for this node in this interval ?
Yes
No
ST5
Compute node average request count per interval
ST4
Stop
ST6
Compute limit as a percentage of the average
ST 7
current interval request count > limit ?
No
Yes
ST8
Generate security event

FiG · 17A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

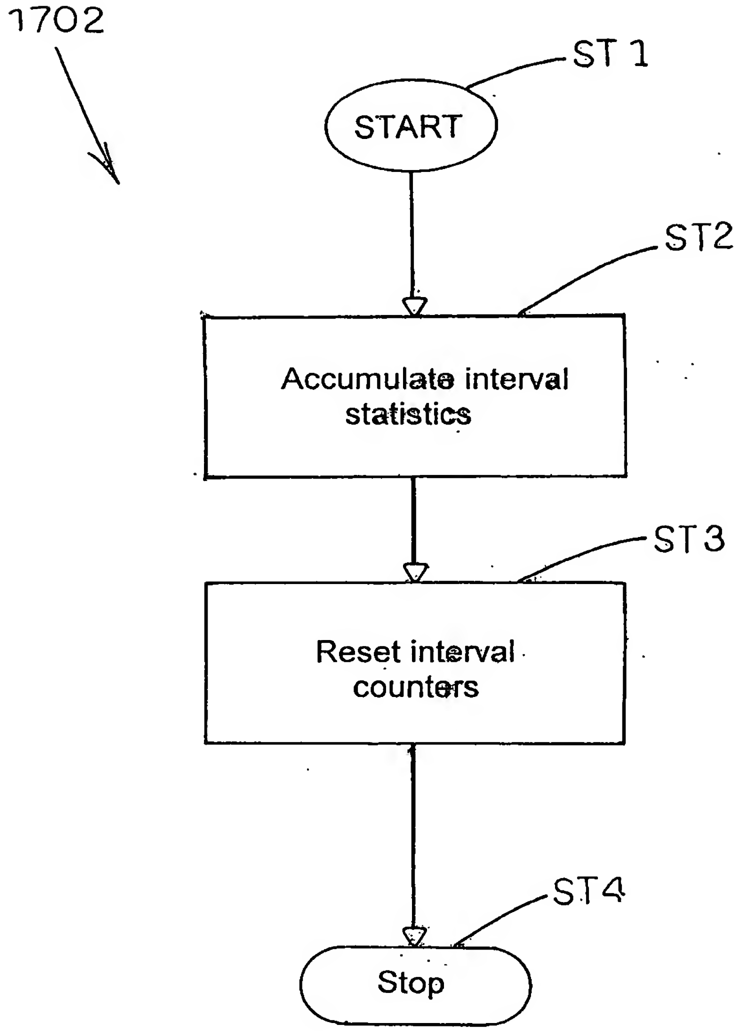


FIG. 17B

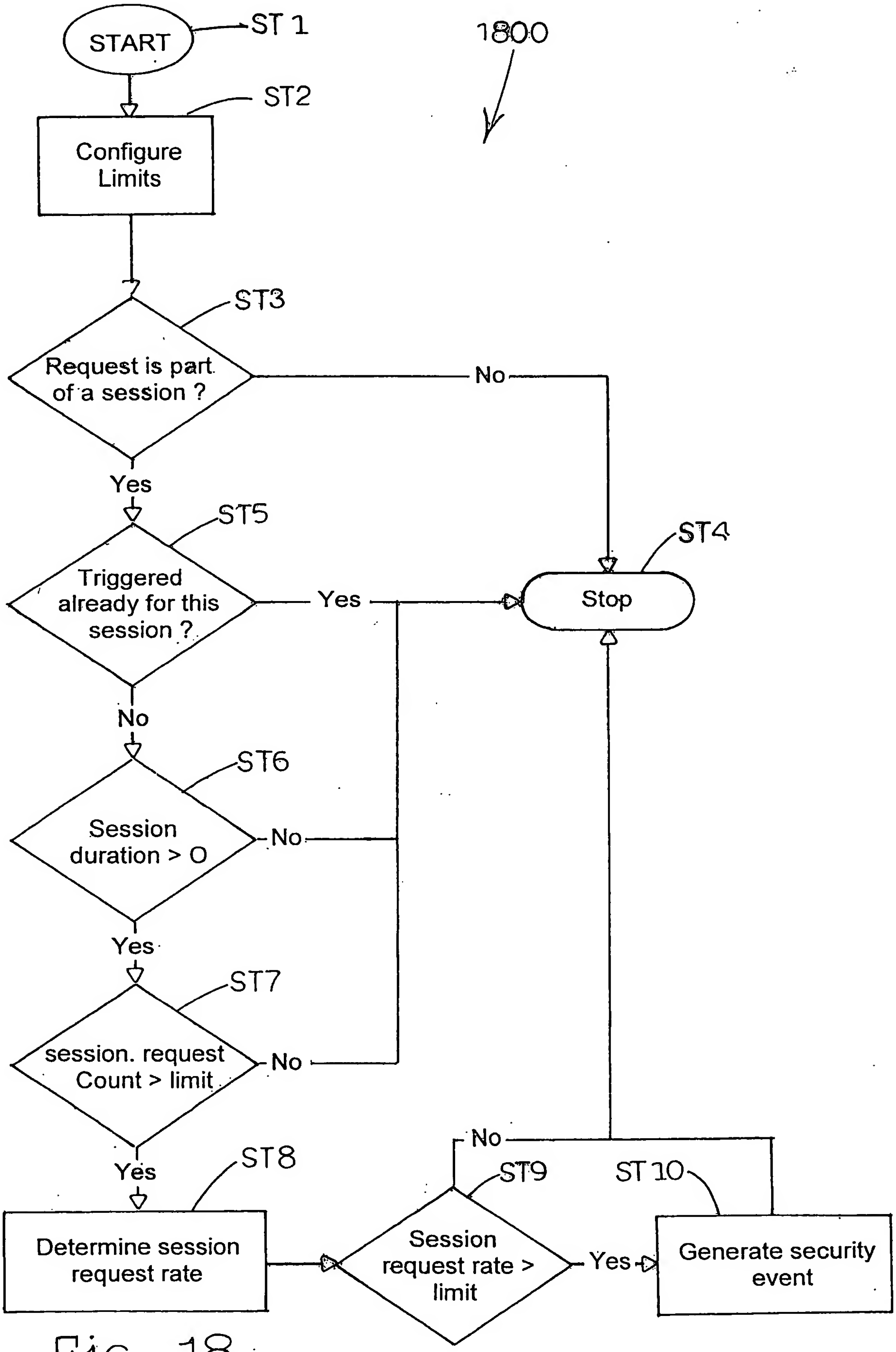

1800
START
ST 1
Configure Limits
ST2
Request is part of a session ?
ST3
No
Yes
Triggered already for this session ?
ST5
Yes
Stop
ST4
No
Session duration > O
ST6
No
Yes
session. request Count > limit
ST7
No
Yes
Determine session request rate
ST8
Session request rate > limit
ST9
No
Yes
Generate security event
ST 10

FiG · 18

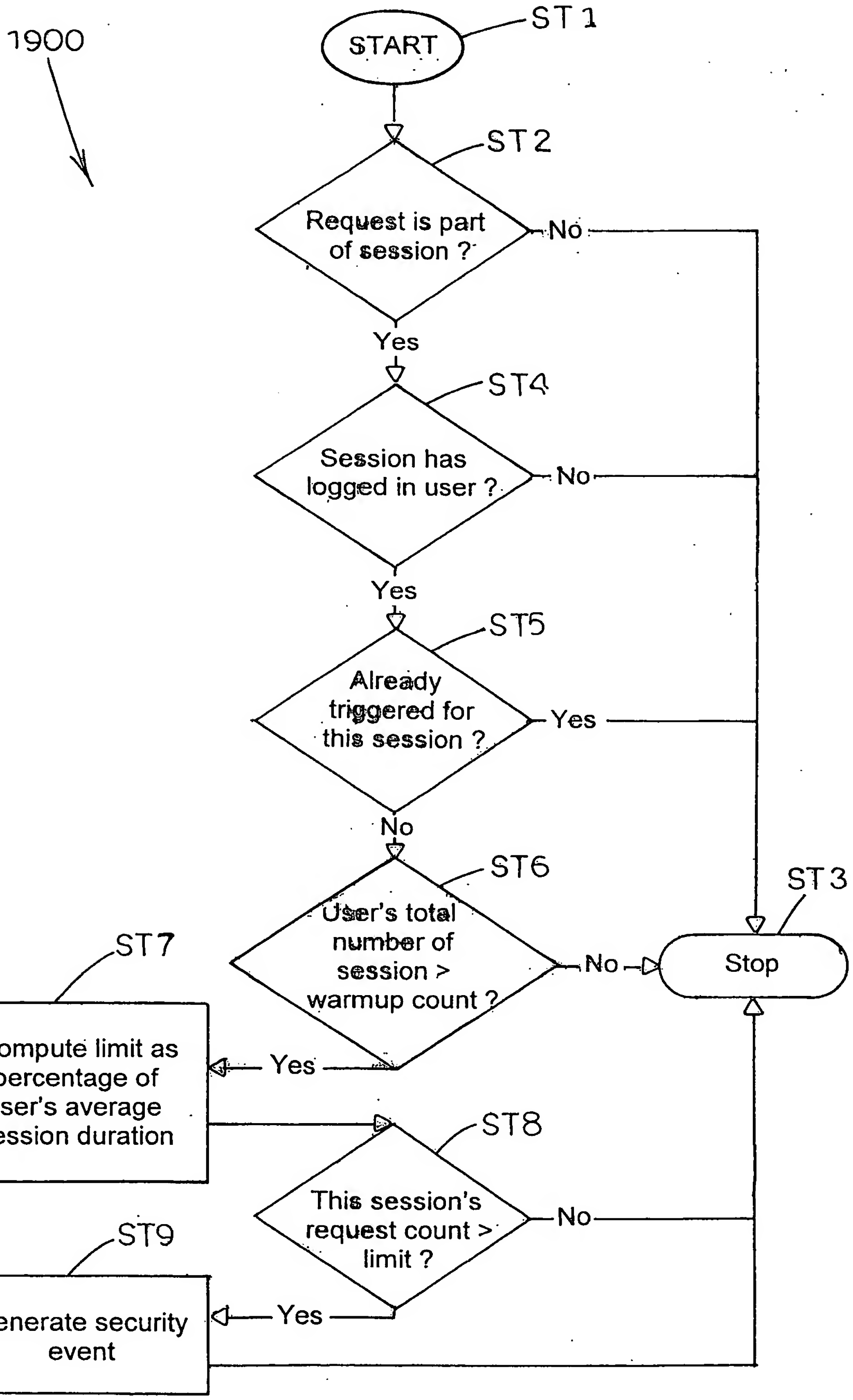

1900
START
ST 1
ST 2
Request is part of session ?
No
Yes
ST4
Session has logged in user ?
No
Yes
ST5
Already triggered for this session ?
Yes
No
ST6
User's total number of session > warmup count ?
No
ST 3
Stop
ST7
Compute limit as percentage of user's average session duration
Yes
ST8
This session's request count > limit ?
No
ST9
Generate security event
Yes

FiG · 19A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

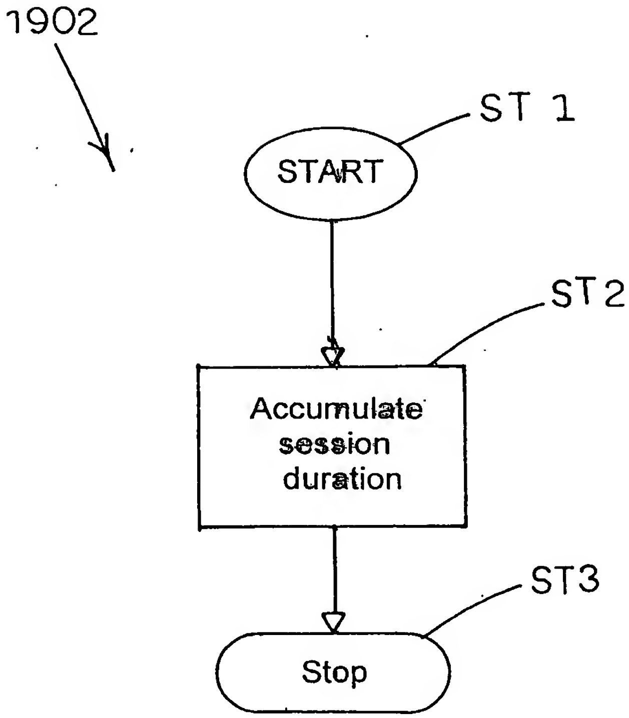


Fig · 19B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

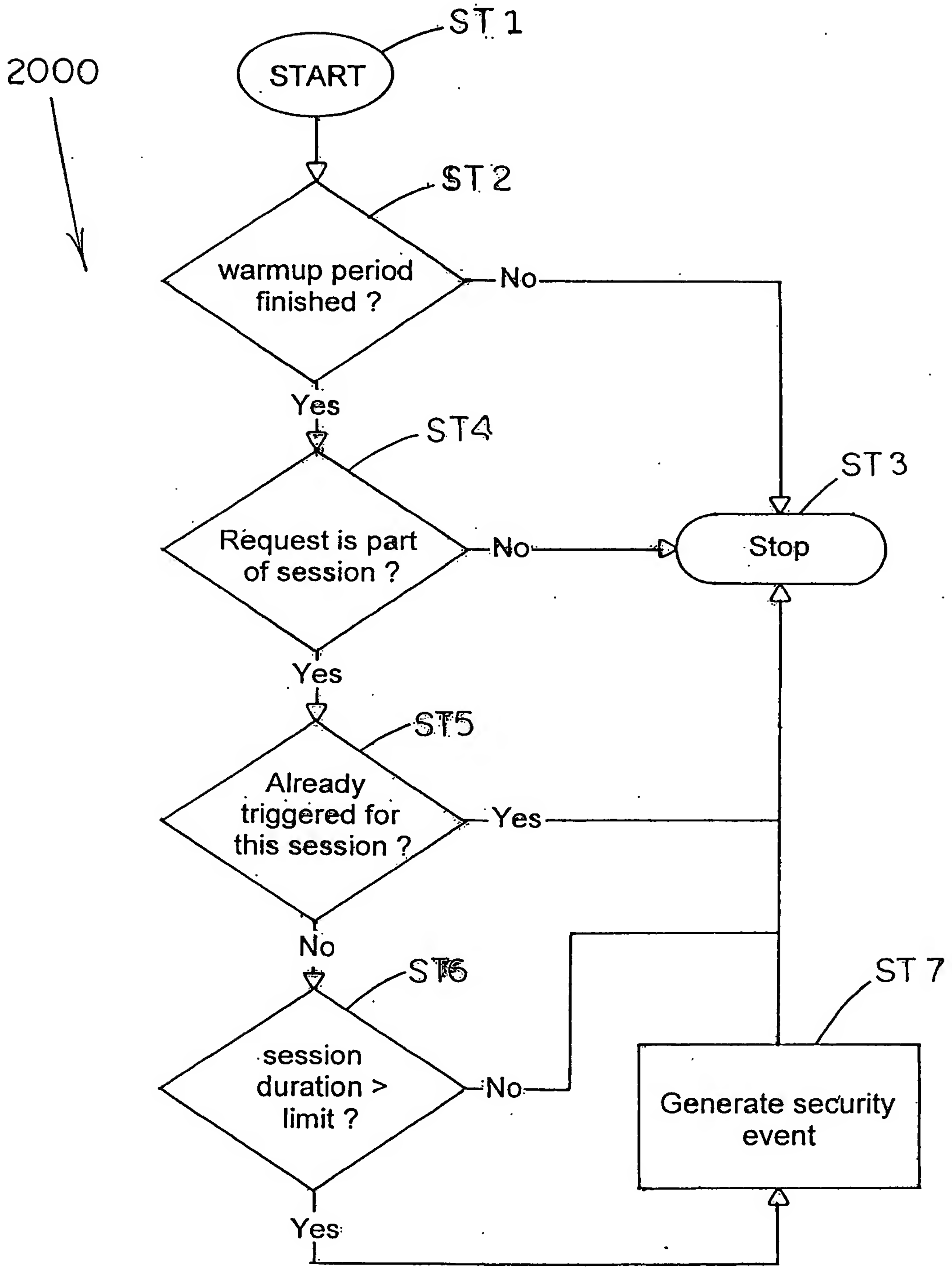


FiG · 20A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

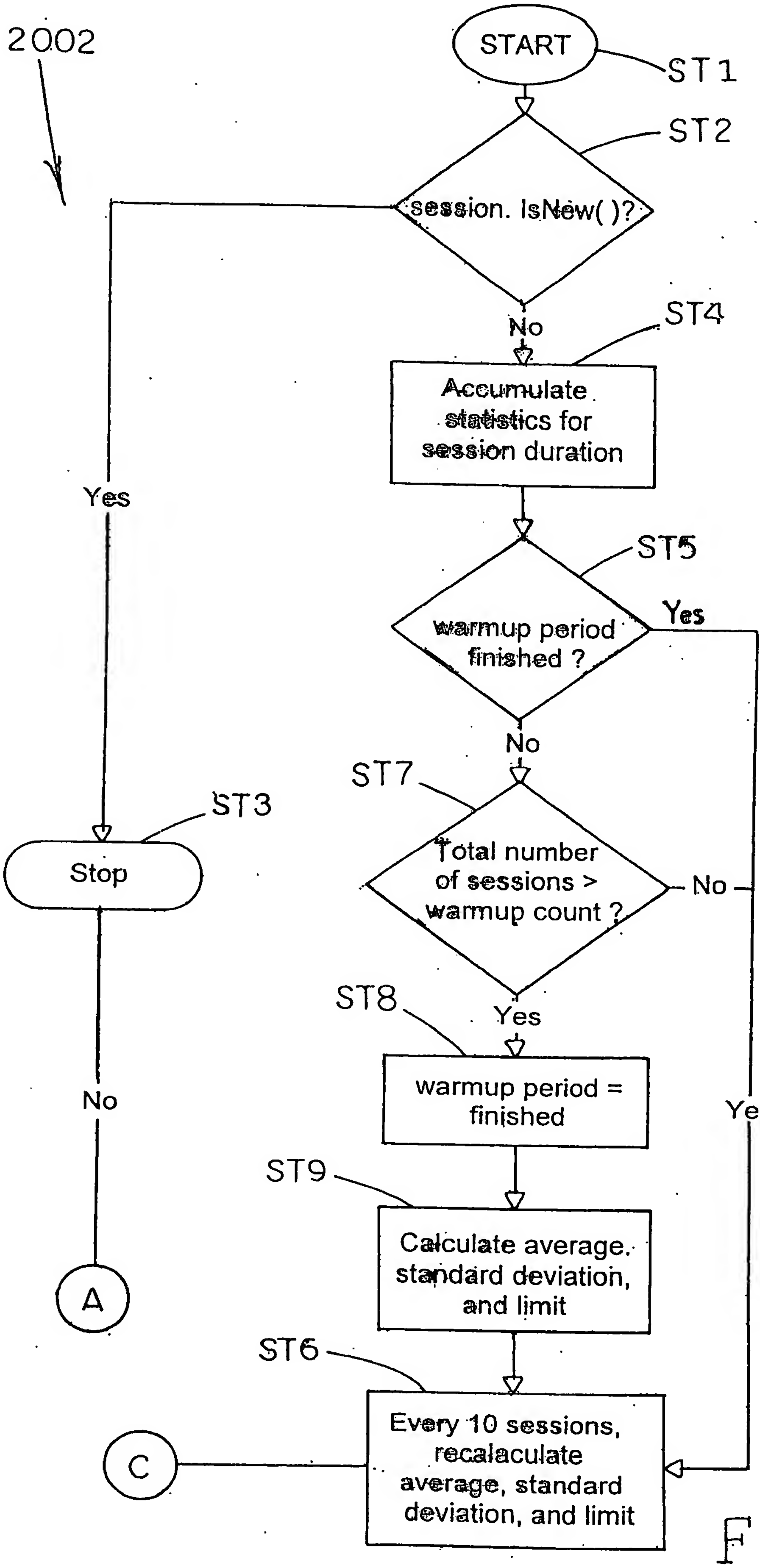

2002
START
ST1
ST2
session. IsNew( )?
No
ST4
Accumulate statistics for session duration
Yes
ST5
Yes
warmup period finished ?
No
ST7
ST3
Total number of sessions > warmup count ?
No
Stop
ST8
Yes
warmup period = finished
No
Yes
ST9
Calculate average, standard deviation, and limit
A
ST6
Every 10 sessions, recalaculate average, standard deviation, and limit
C

FIG. 20B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

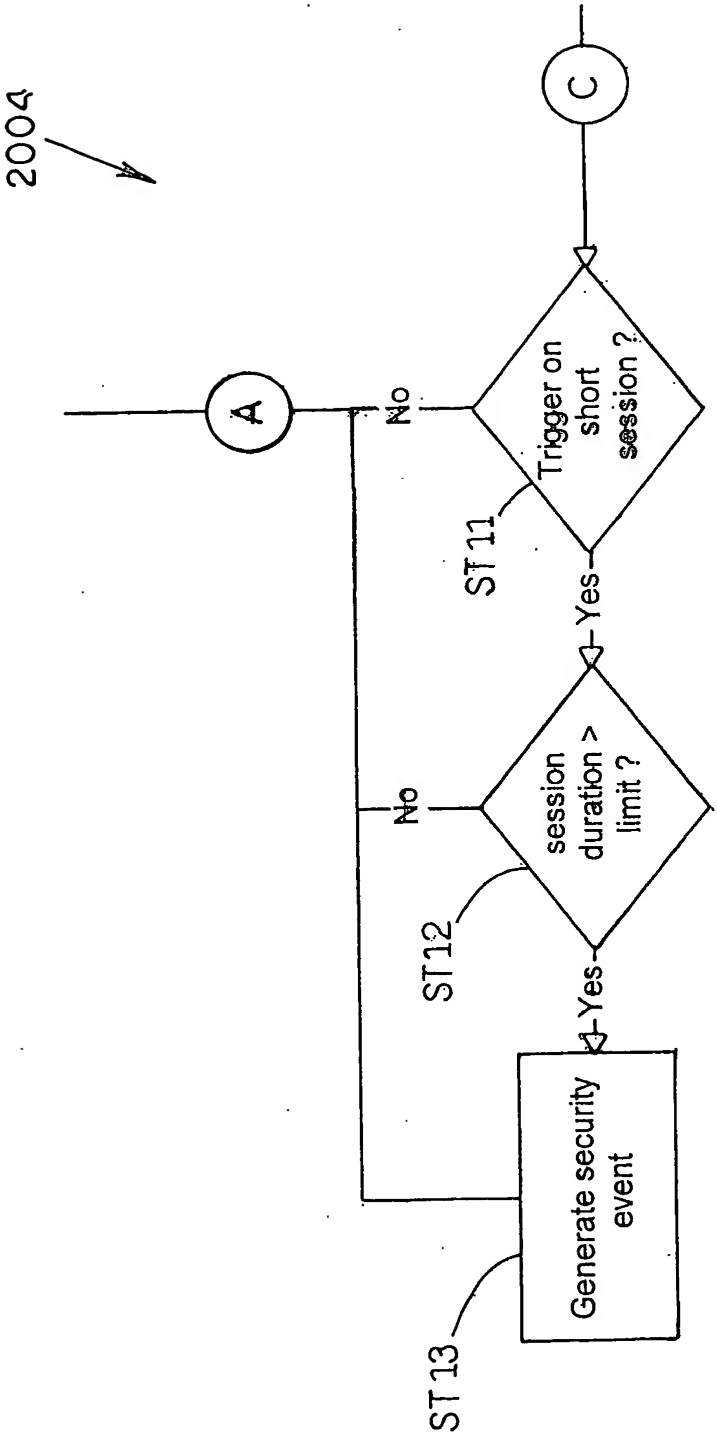


Fig. 20C

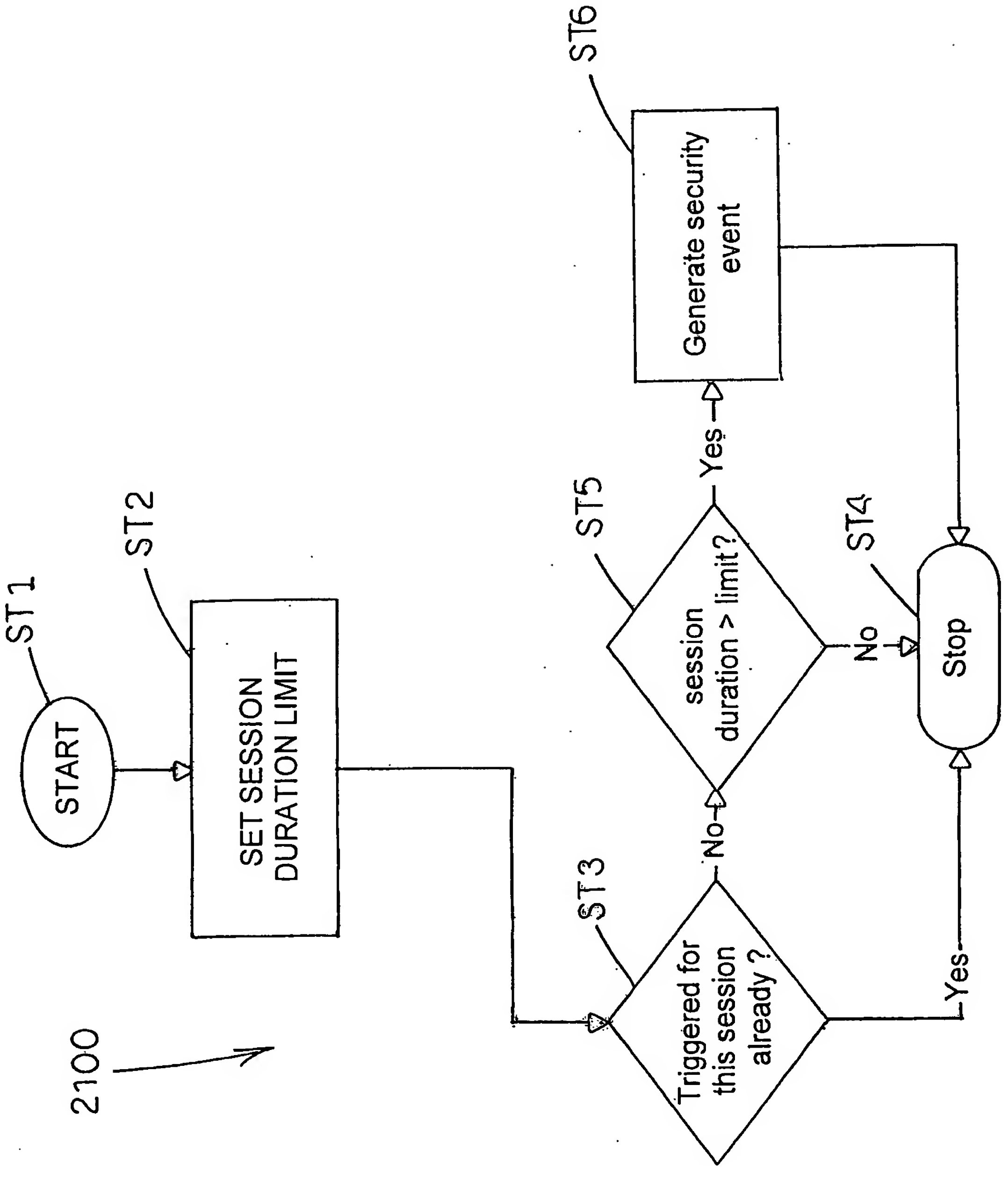

2100
ST1
START
ST2
SET SESSION DURATION LIMIT
ST3
Triggered for this session already ?
Yes
No
ST5
session duration > limit?
No
Yes
ST4
Stop
ST6
Generate security event

FiG. 21

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

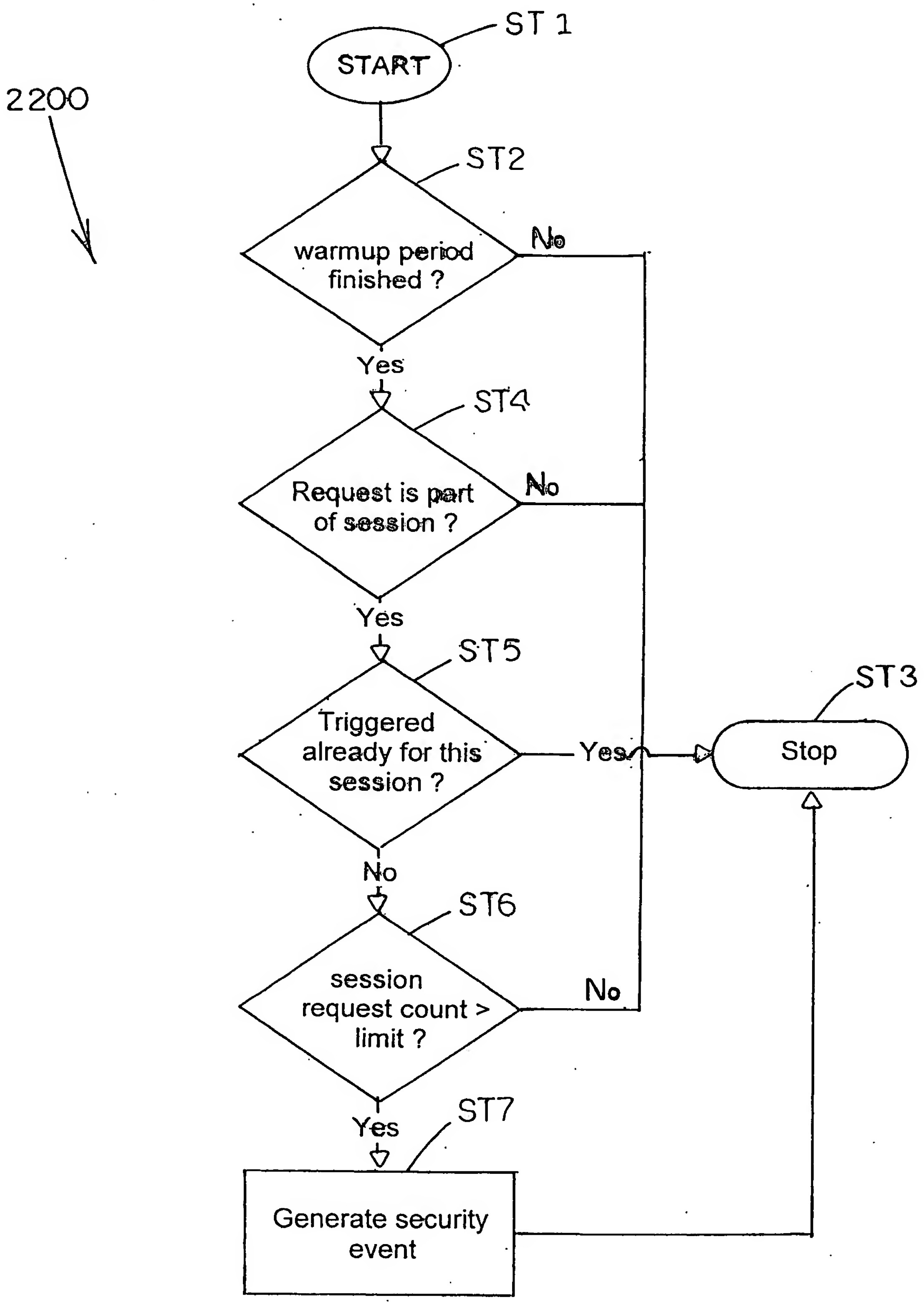


Fig. 22A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

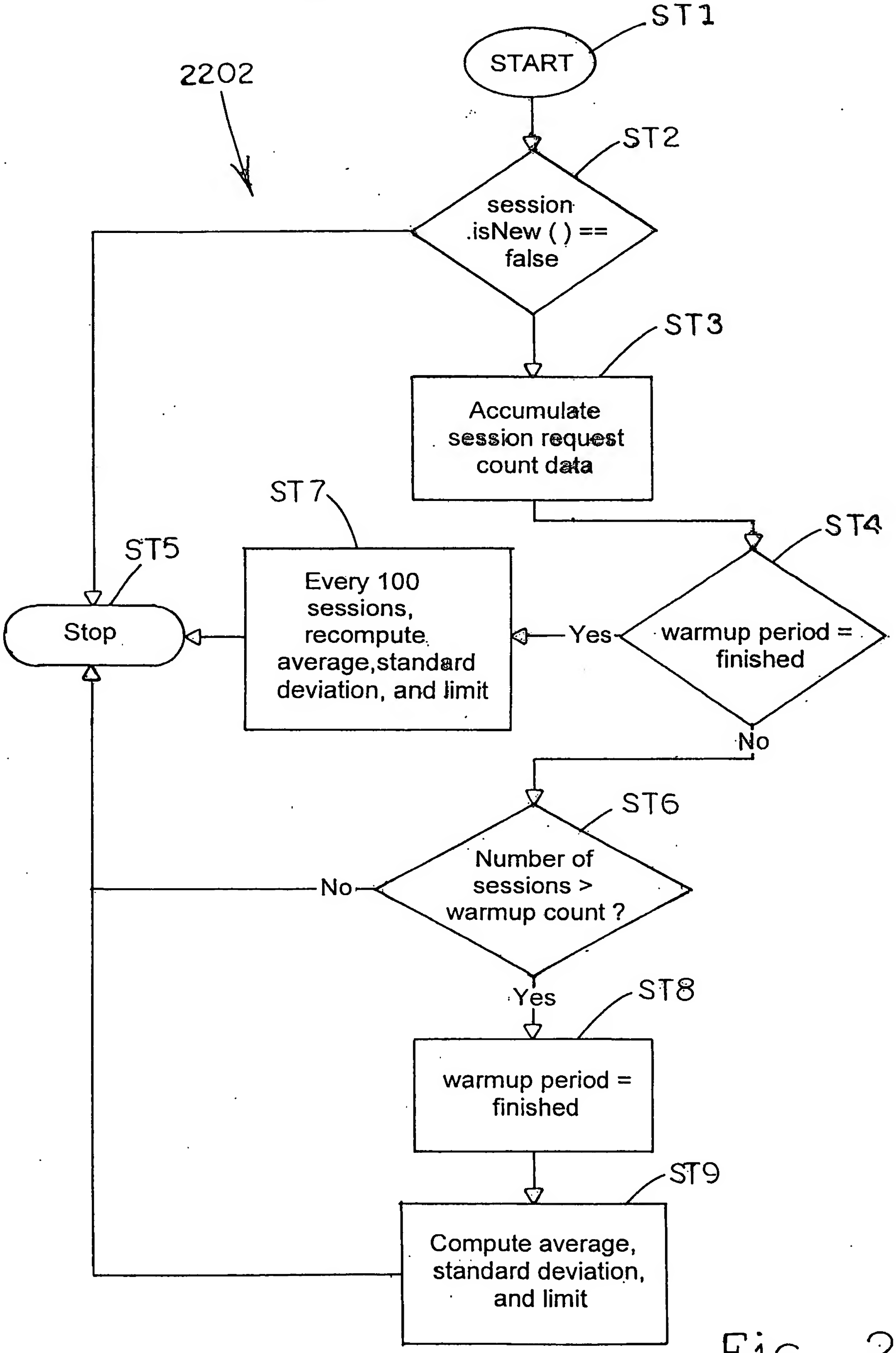

ST1
START
2202
ST2
session .isNew ( ) == false
ST3
Accumulate session request count data
ST7
ST4
ST5
Every 100 sessions, recompute average,standard deviation, and limit
Stop
Yes
warmup period = finished
No
ST6
No
Number of sessions > warmup count ?
Yes
ST8
warmup period = finished
ST9
Compute average, standard deviation, and limit

Fig. 22B

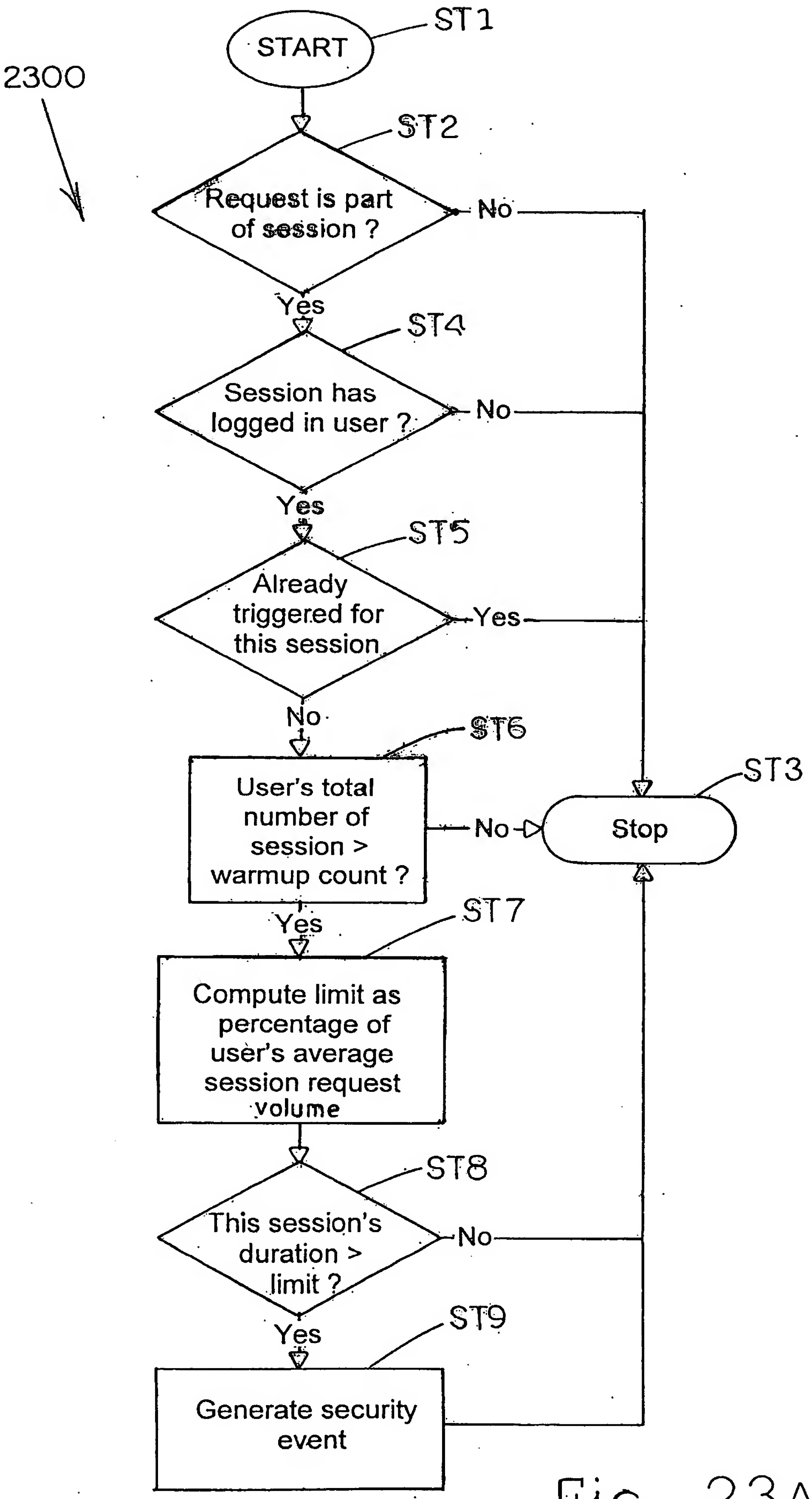

2300
START
ST1
ST2
Request is part of session ?
No
Yes
ST4
Session has logged in user ?
No
Yes
ST5
Already triggered for this session
Yes
No
ST6
User's total number of session > warmup count ?
No
Stop
ST3
Yes
ST7
Compute limit as percentage of user's average session request volume
ST8
This session's duration > limit ?
No
Yes
ST9
Generate security event

FiG · 23A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

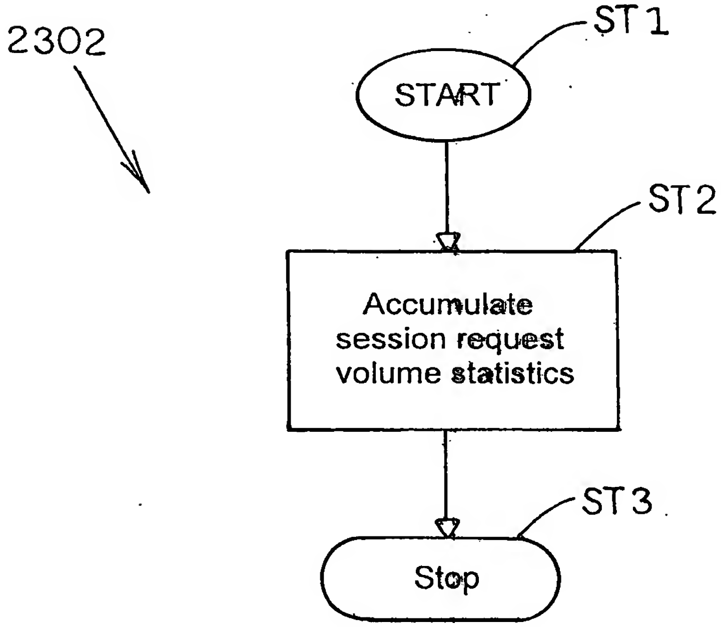
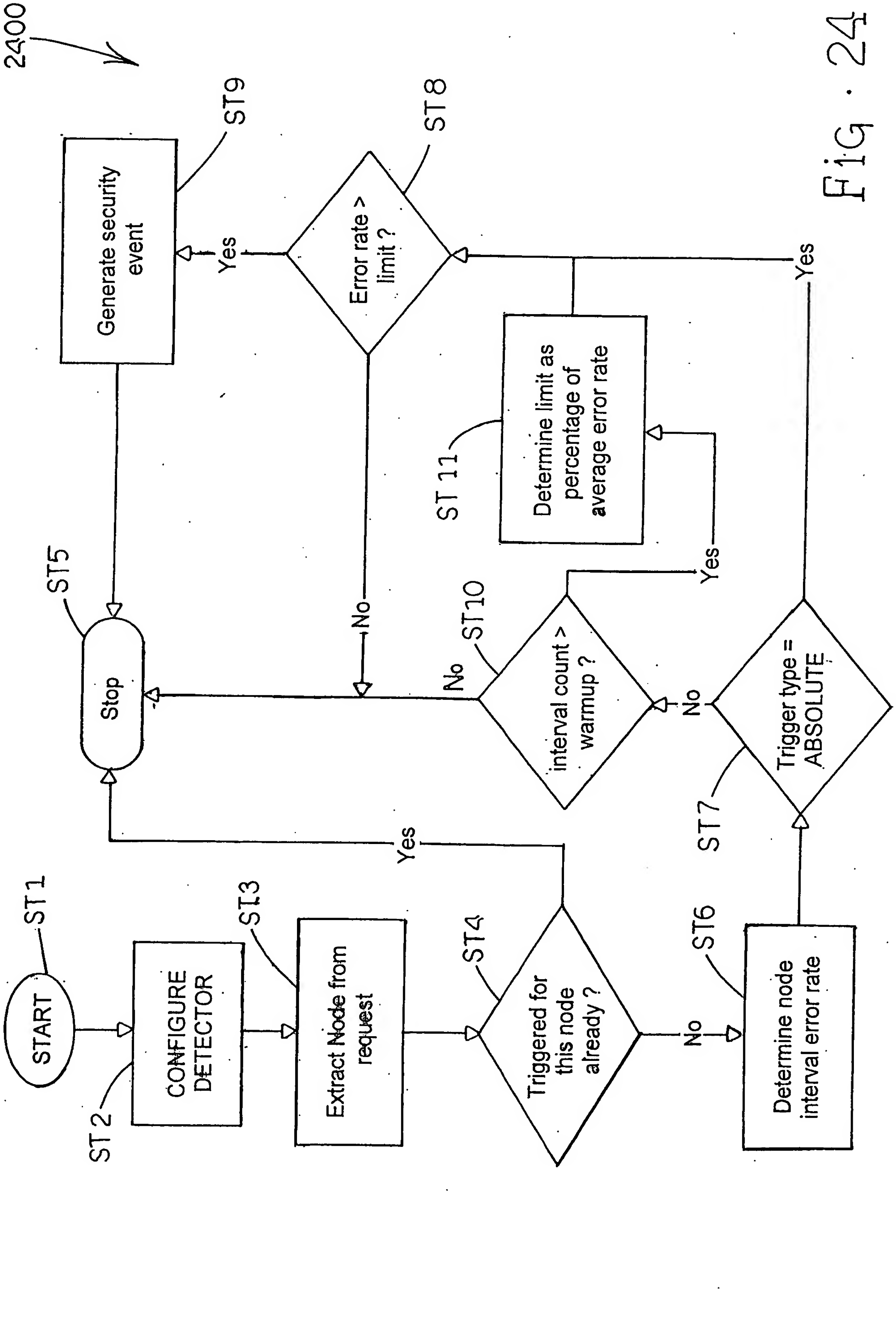


Fig. 23B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6



2400
START
ST 1
CONFIGURE DETECTOR
ST 2
Extract Node from request
ST3
Triggered for this node already ?
ST4
Yes
No
Determine node interval error rate
ST6
Trigger type = ABSOLUTE
ST 7
No
Yes
interval count > warmup ?
ST10
No
Yes
Determine limit as percentage of average error rate
ST 11
Error rate > limit ?
ST 8
Yes
No
Generate security event
ST9
Stop
ST5

Fig. 24

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER
PROGRAM PRODUCTS FOR MONITORING A
SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

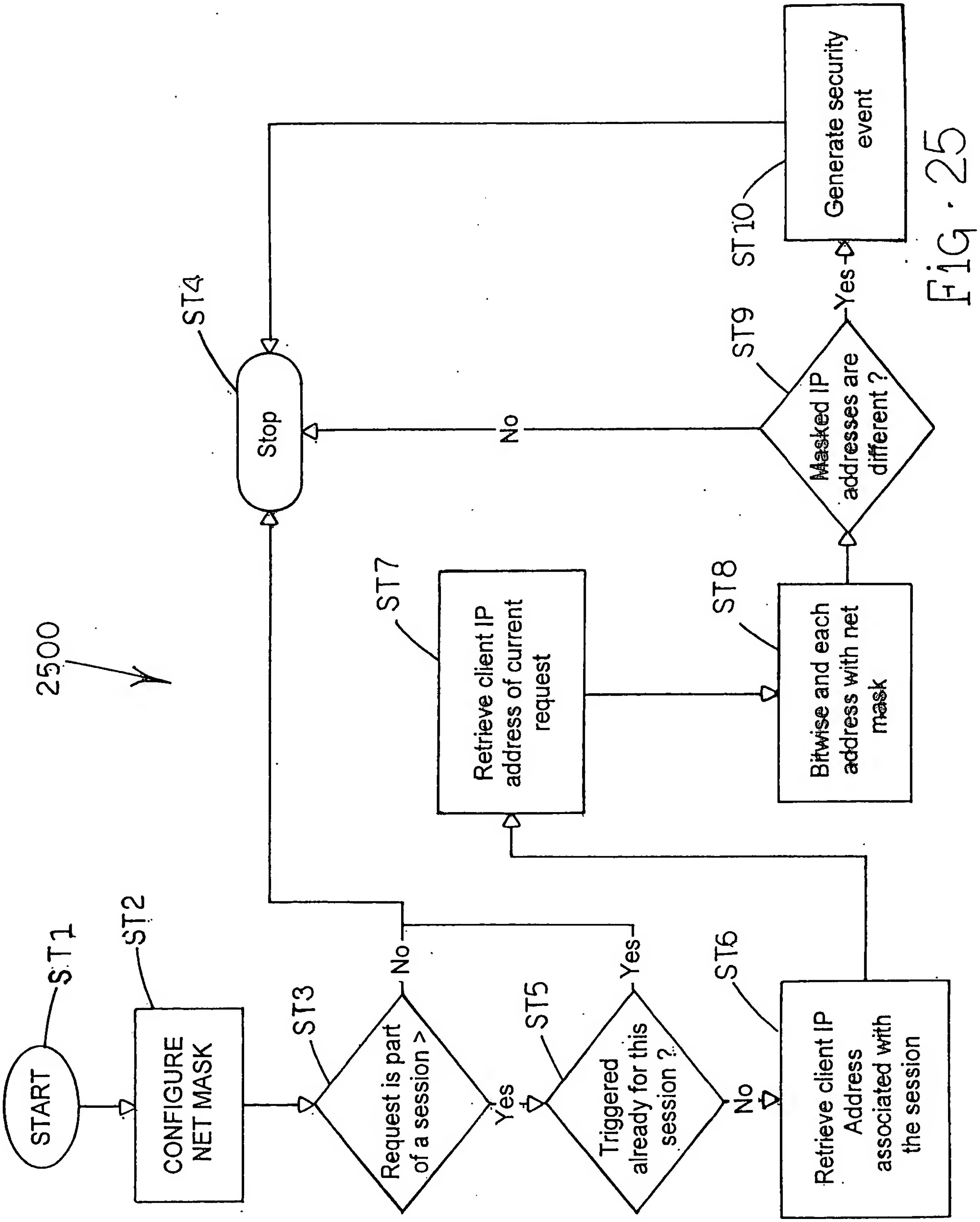

2500
START
ST1
CONFIGURE NET MASK
ST2
Request is part of a session >
ST3
Yes
No
Triggered already for this session ?
ST5
Yes
No
Retrieve client IP Address associated with the session
ST6
Stop
ST4
Retrieve client IP address of current request
ST7
Bitwise and each address with net mask
ST8
Masked IP addresses are different ?
ST9
No
Yes
Generate security event
ST10

FIG. 25

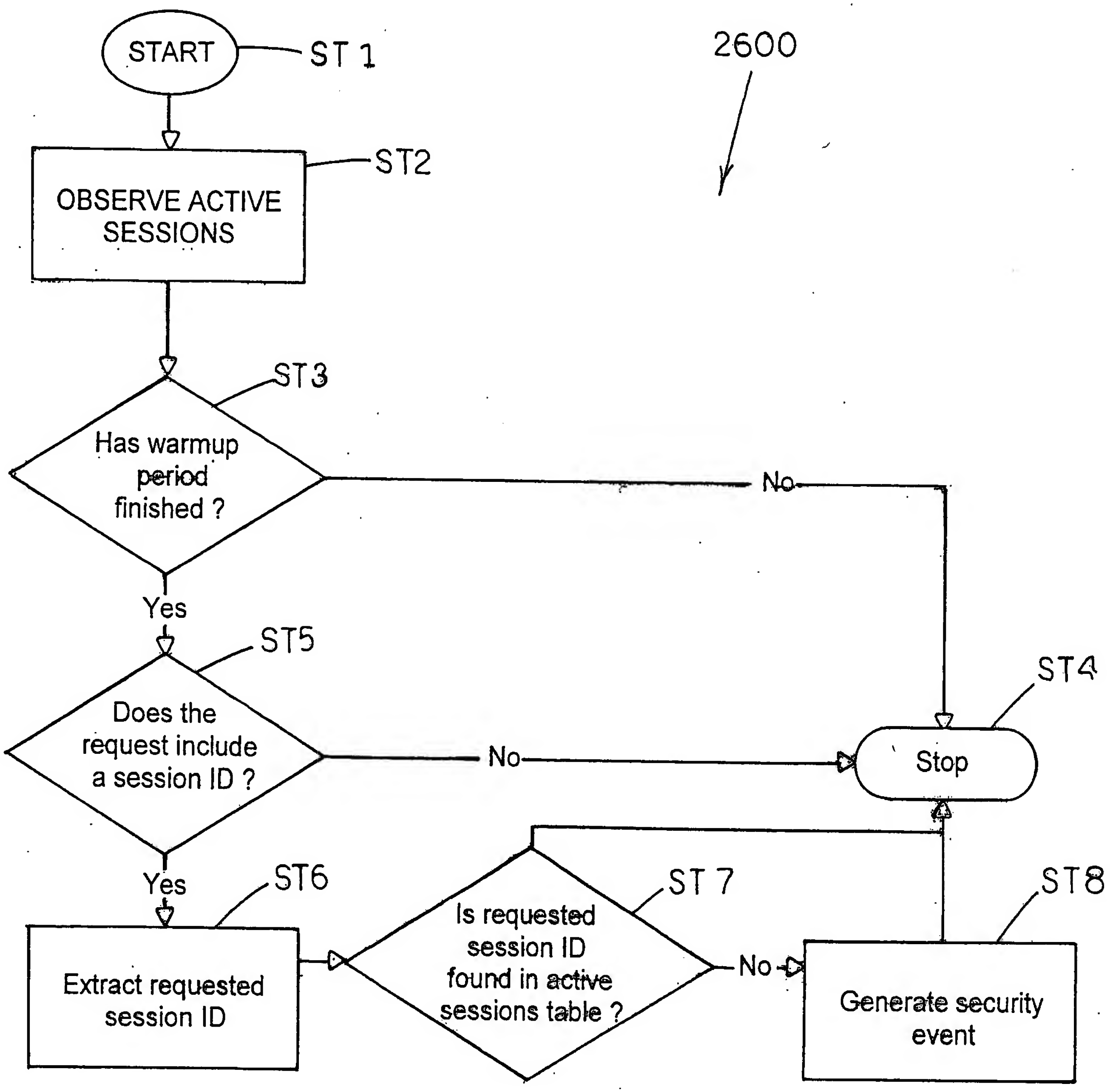
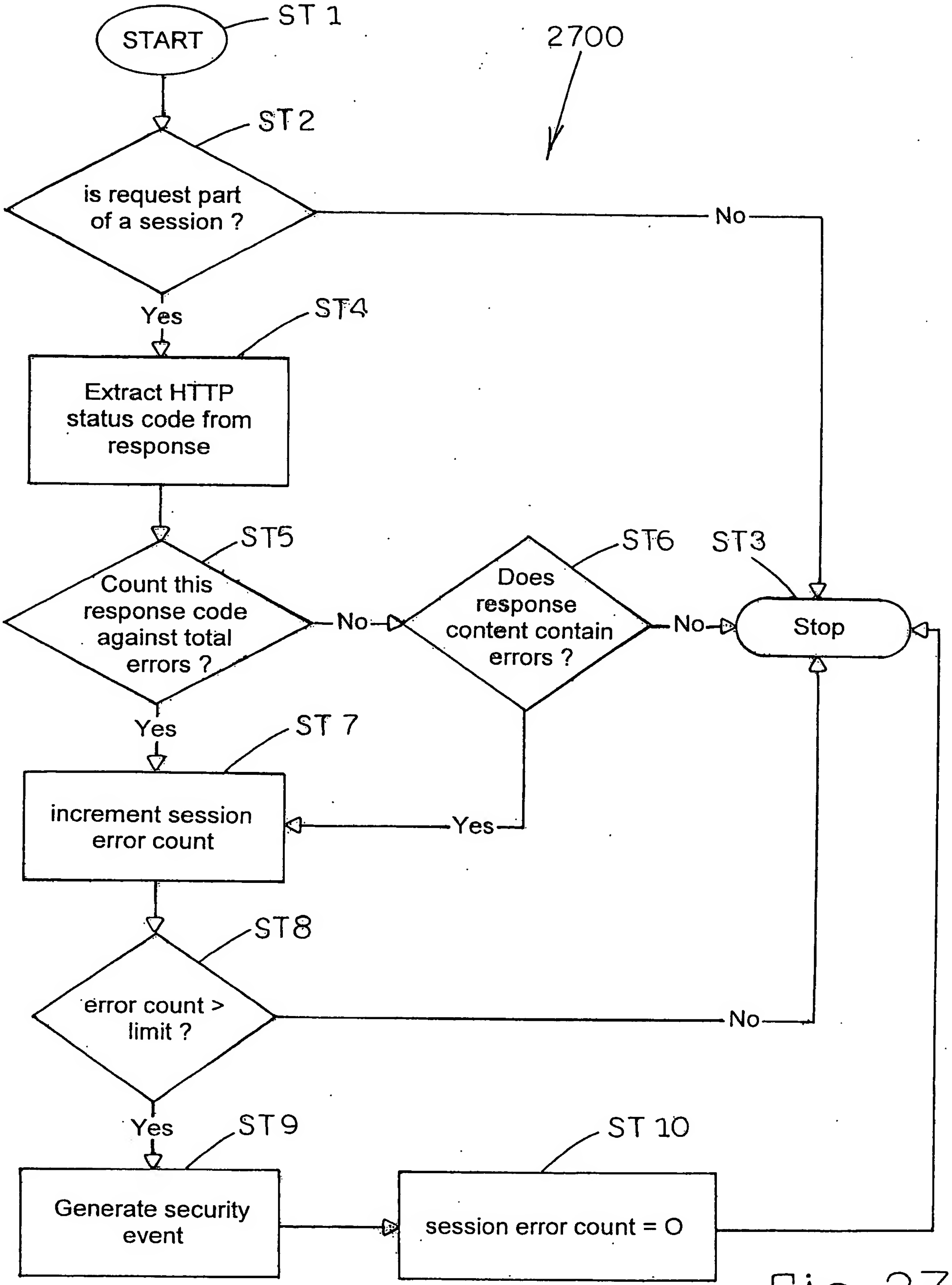

2600
START
ST 1
OBSERVE ACTIVE SESSIONS
ST2
Has warmup period finished ?
ST3
No
Yes
Does the request include a session ID ?
ST5
No
Yes
Extract requested session ID
ST6
Is requested session ID found in active sessions table ?
ST 7
No
Generate security event
ST8
Stop
ST4

FIG. 26

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6


START
ST 1
2700
ST2
is request part of a session ?
No
Yes
ST4
Extract HTTP status code from response
ST5
Count this response code against total errors ?
No
ST6
Does response content contain errors ?
No
ST3
Stop
Yes
ST 7
increment session error count
Yes
ST8
error count > limit ?
No
Yes
ST9
Generate security event
ST 10
session error count = O

Fig·27

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

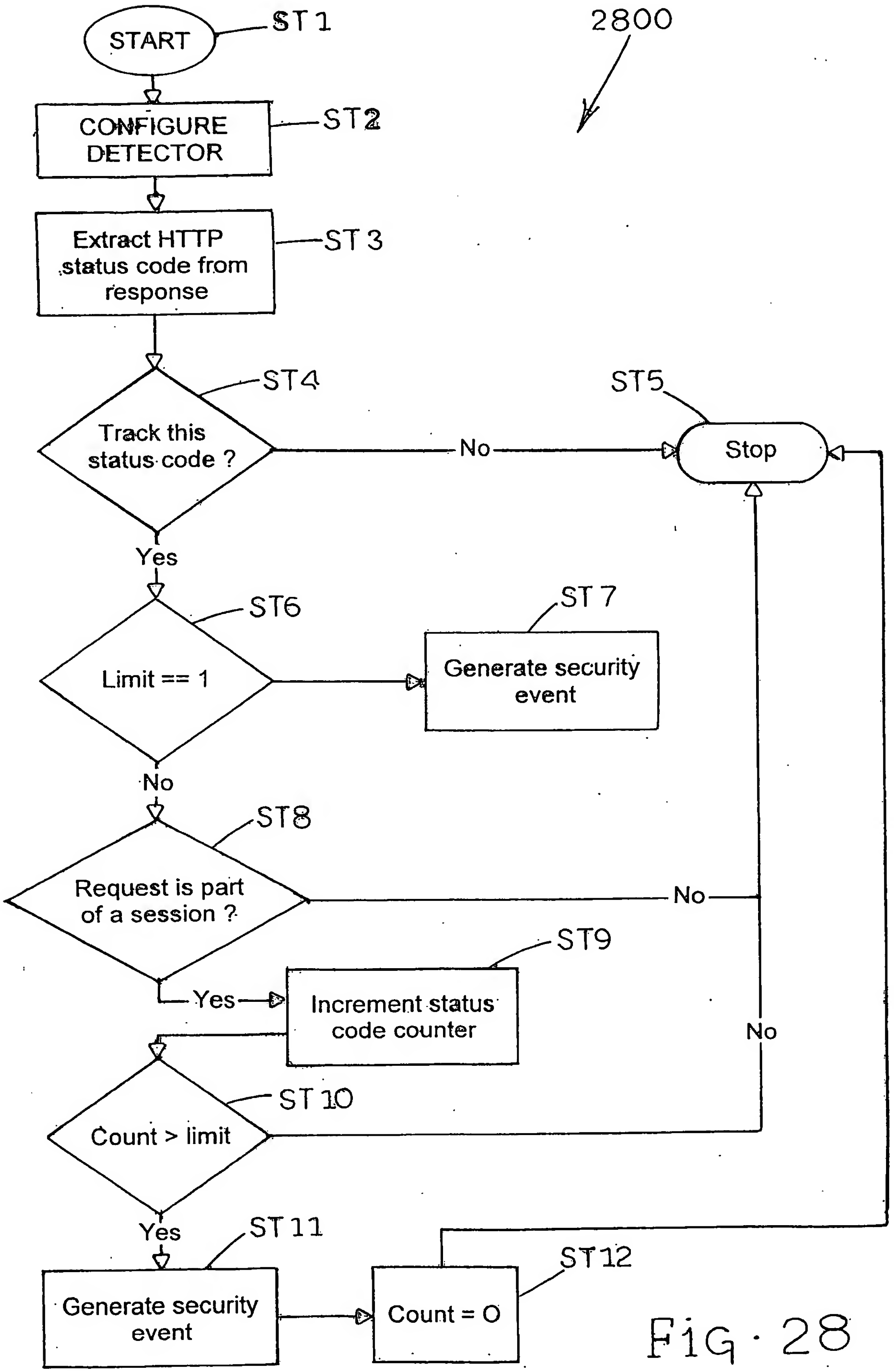


Fig. 28

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

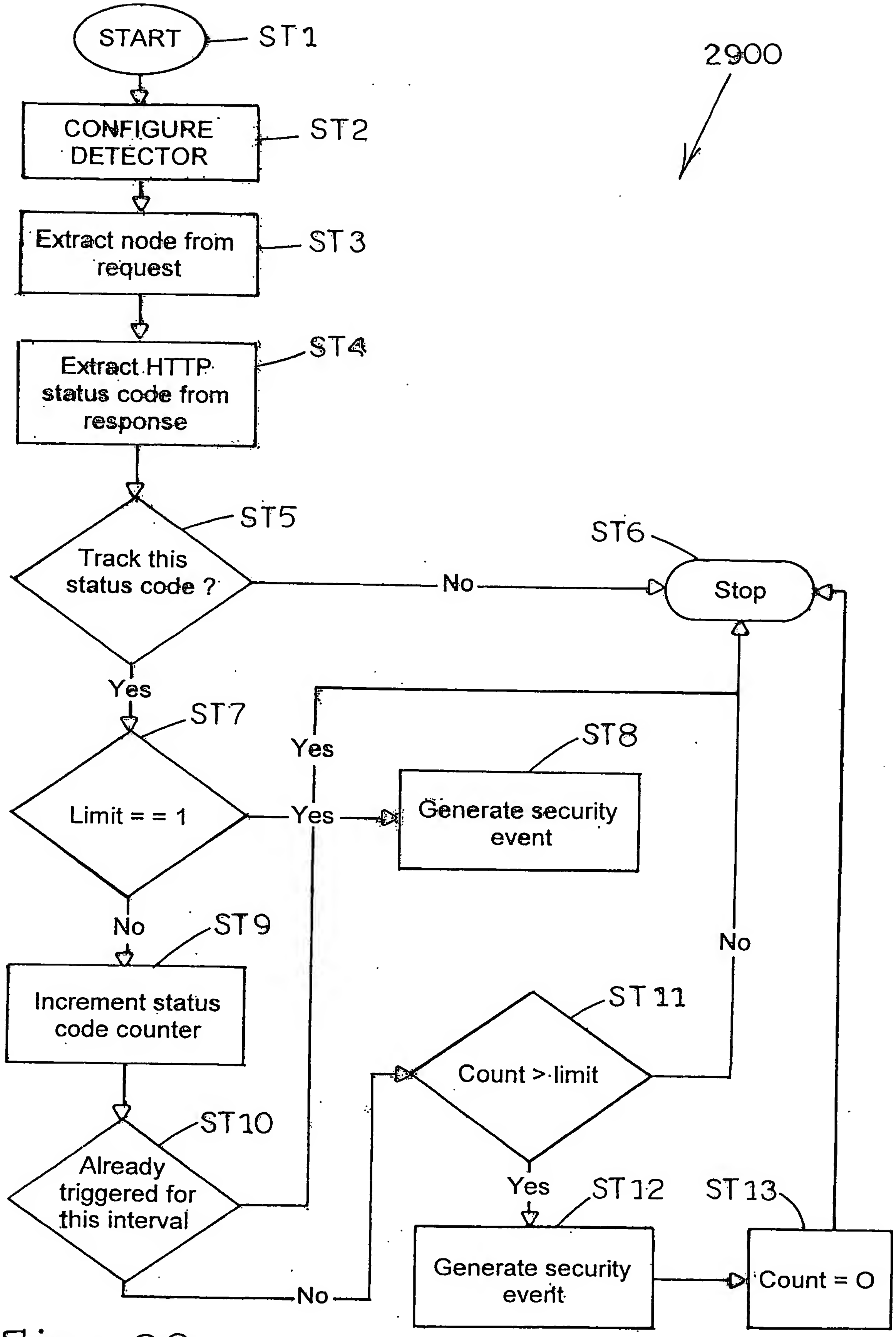
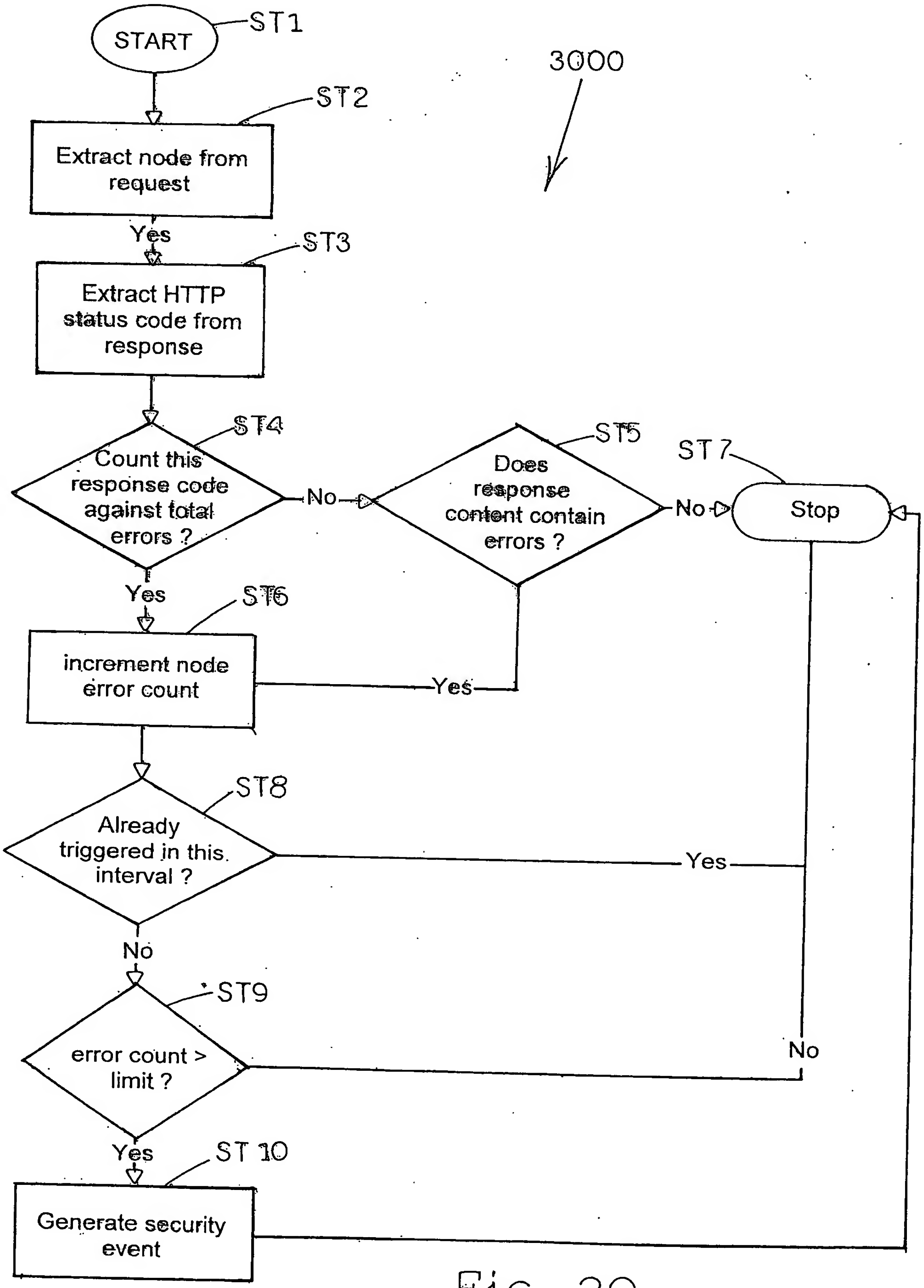


Fig. 29

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6



START
ST1
3000
ST2
Extract node from request
Yes
ST3
Extract HTTP status code from response
ST4
Count this response code against total errors ?
No
ST5
Does response content contain errors ?
No
ST 7
Stop
Yes
ST6
increment node error count
Yes
ST8
Already triggered in this interval ?
Yes
No
ST9
error count > limit ?
No
Yes
ST 10
Generate security event

FiG. 30

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

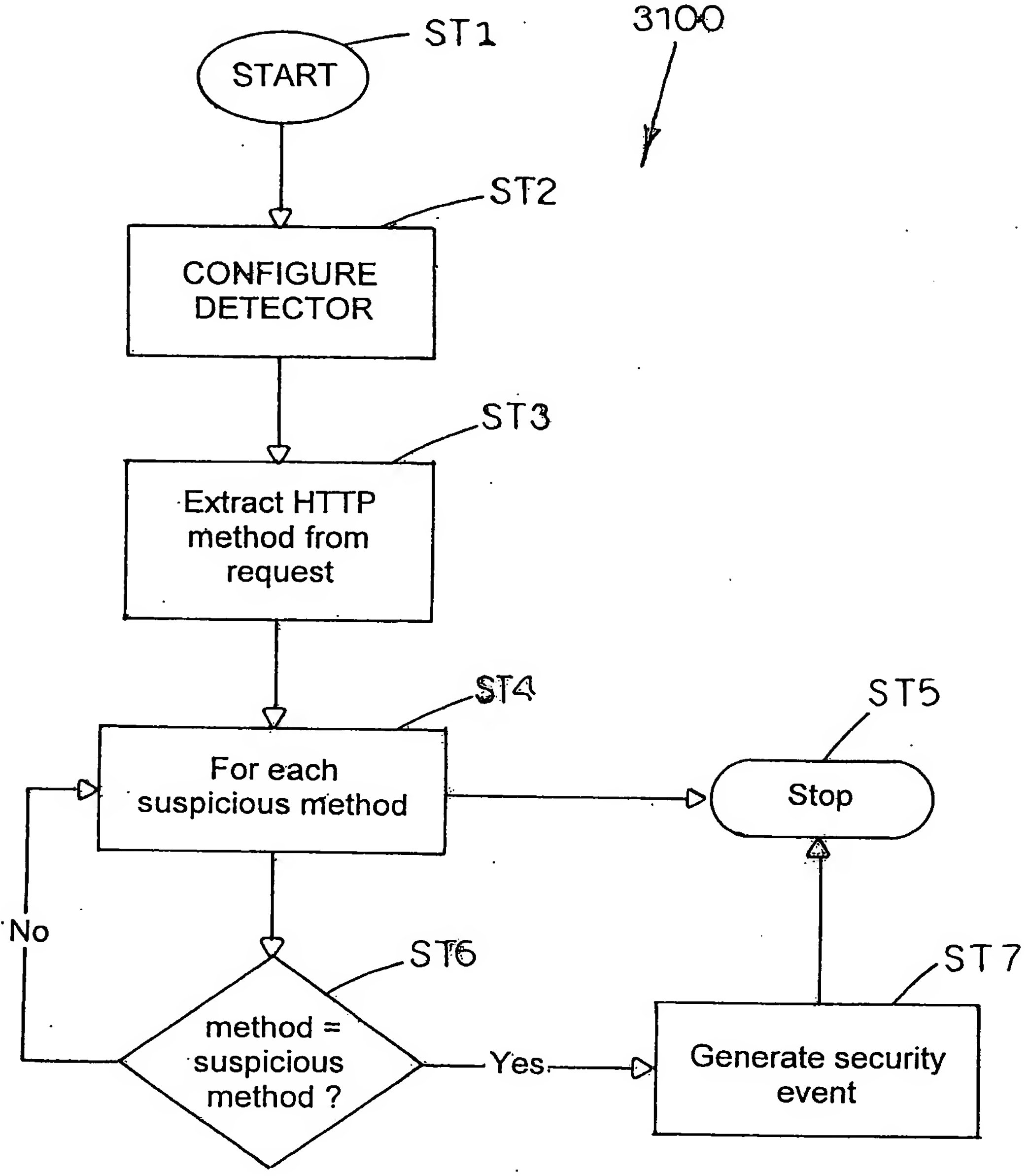

3100
ST1
START
ST2
CONFIGURE DETECTOR
ST3
Extract HTTP method from request
ST4
For each suspicious method
ST5
Stop
No
ST6
method = suspicious method ?
Yes
ST7
Generate security event

Fig · 31

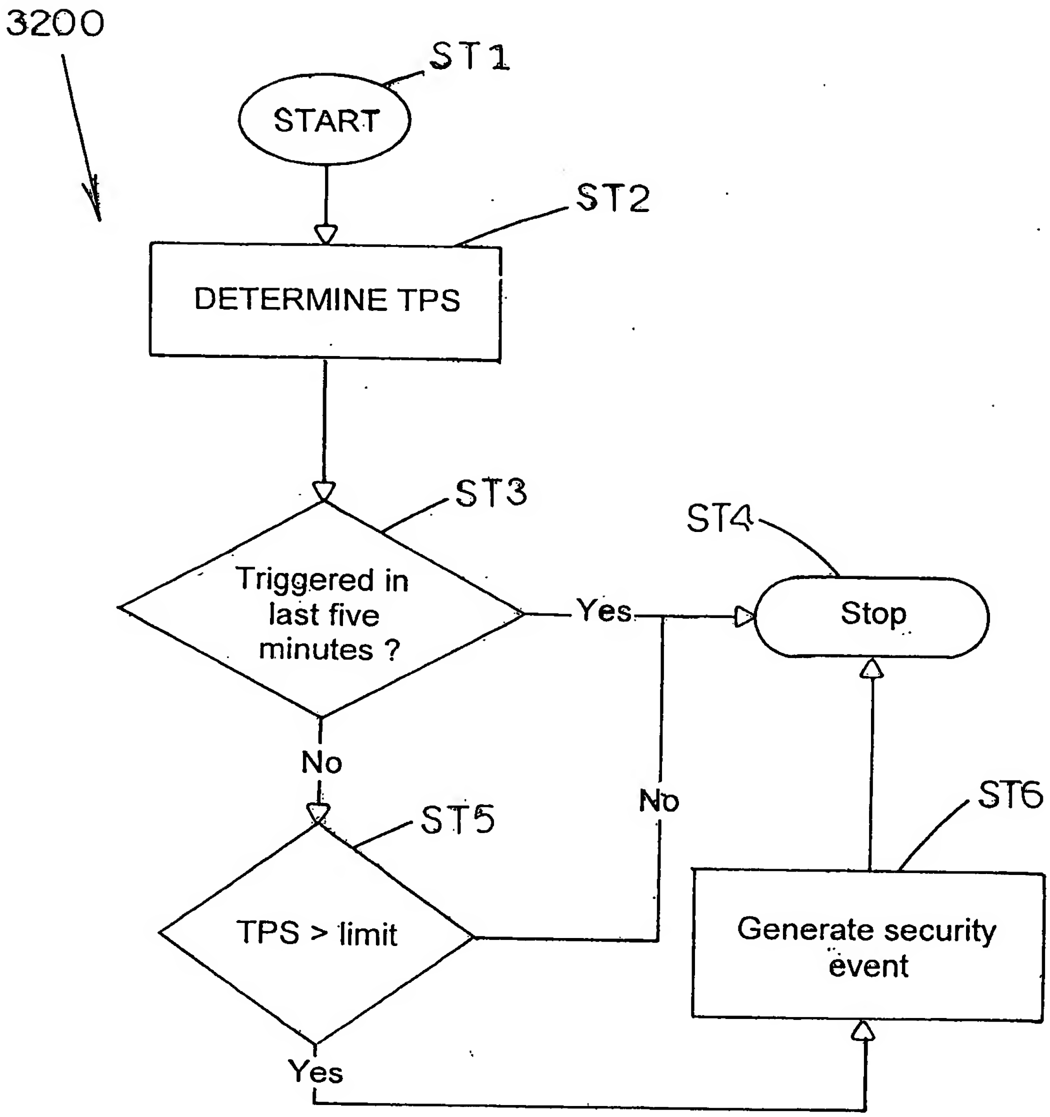

3200
ST1
START
ST2
DETERMINE TPS
ST3
Triggered in last five minutes ?
Yes
ST4
Stop
No
No
ST5
TPS > limit
ST6
Generate security event
Yes

Fig. 32

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

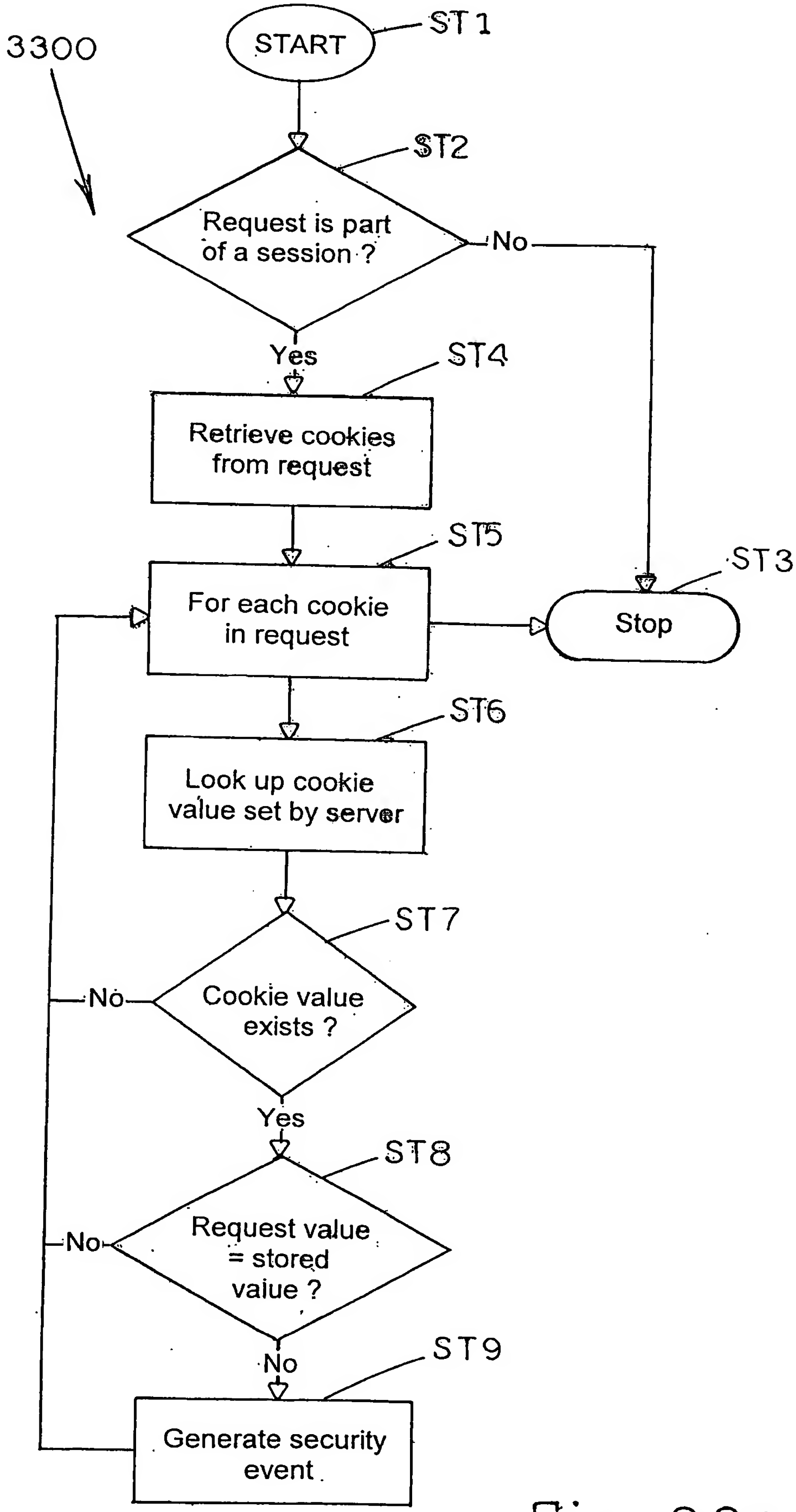

3300
START
ST1
ST2
Request is part of a session ?
No
Yes
ST4
Retrieve cookies from request
ST5
For each cookie in request
ST3
Stop
ST6
Look up cookie value set by server
ST7
No
Cookie value exists ?
Yes
ST8
No
Request value = stored value ?
No
ST9
Generate security event

Fig. 33A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

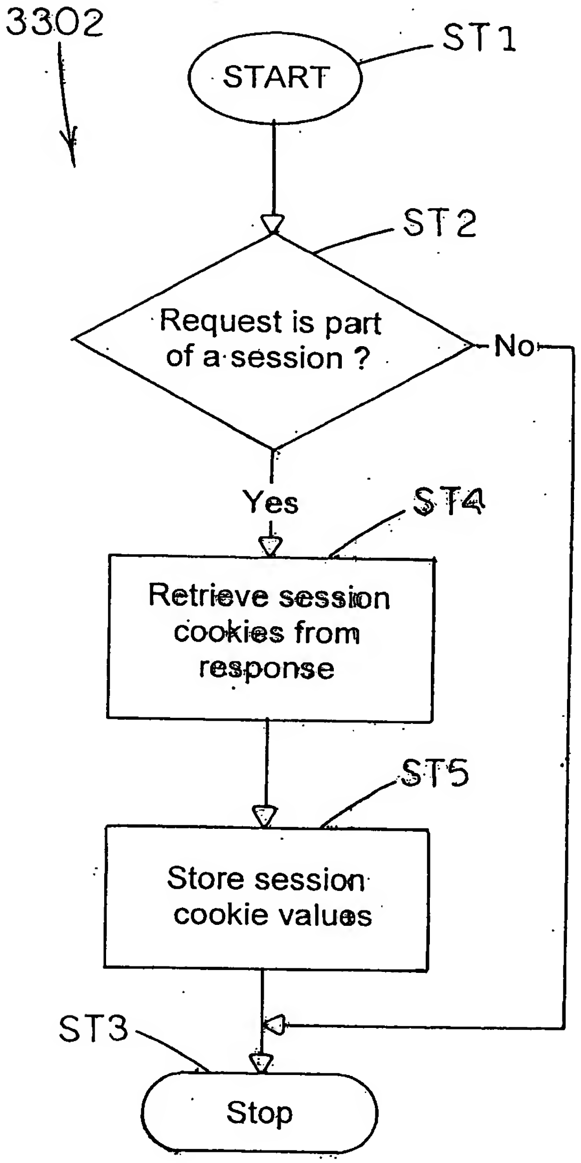

3302
ST1
START
ST2
Request is part of a session ?
No
Yes
ST4
Retrieve session cookies from response
ST5
Store session cookie values
ST3
Stop

FiG · 33B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

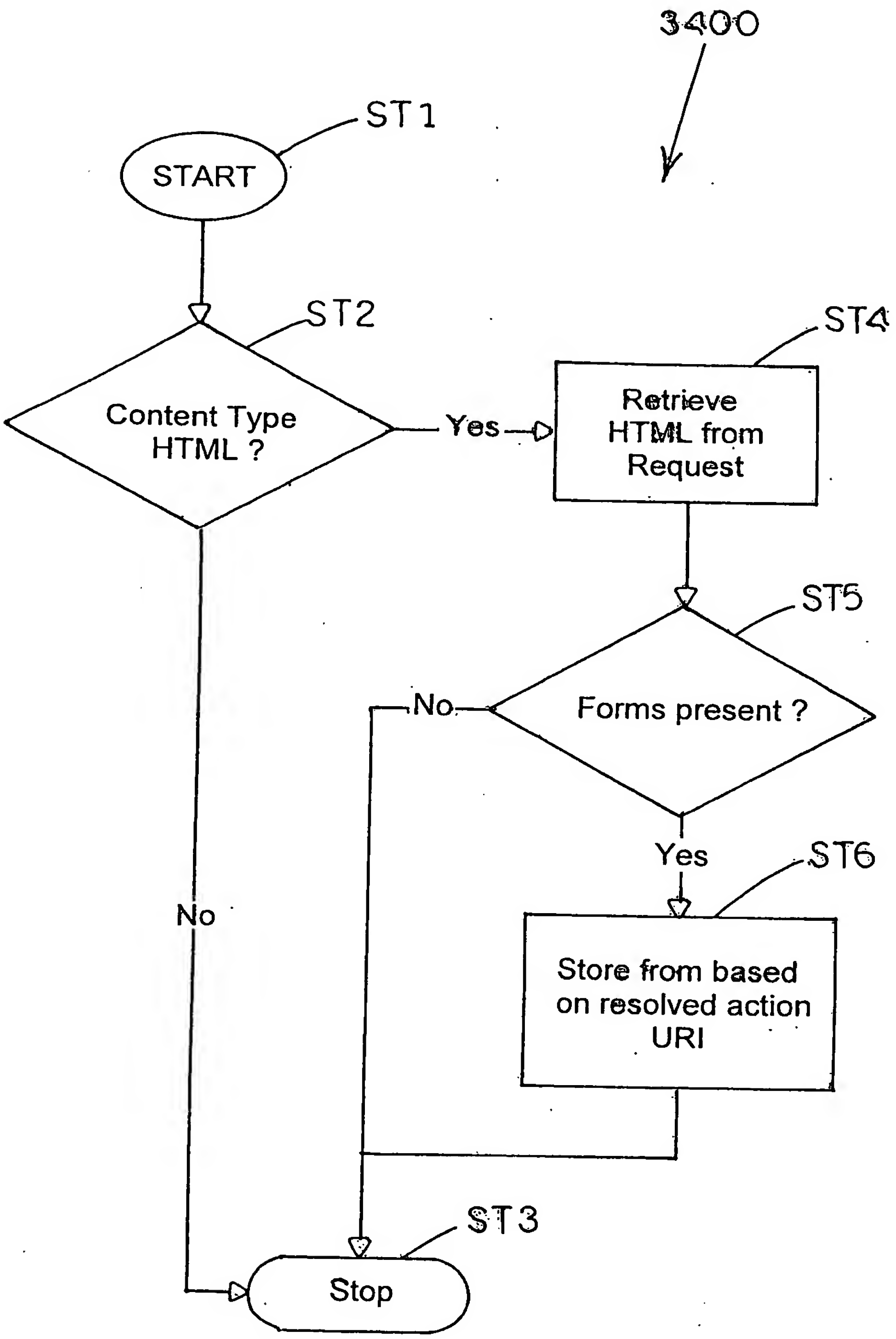


Fig. 34A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

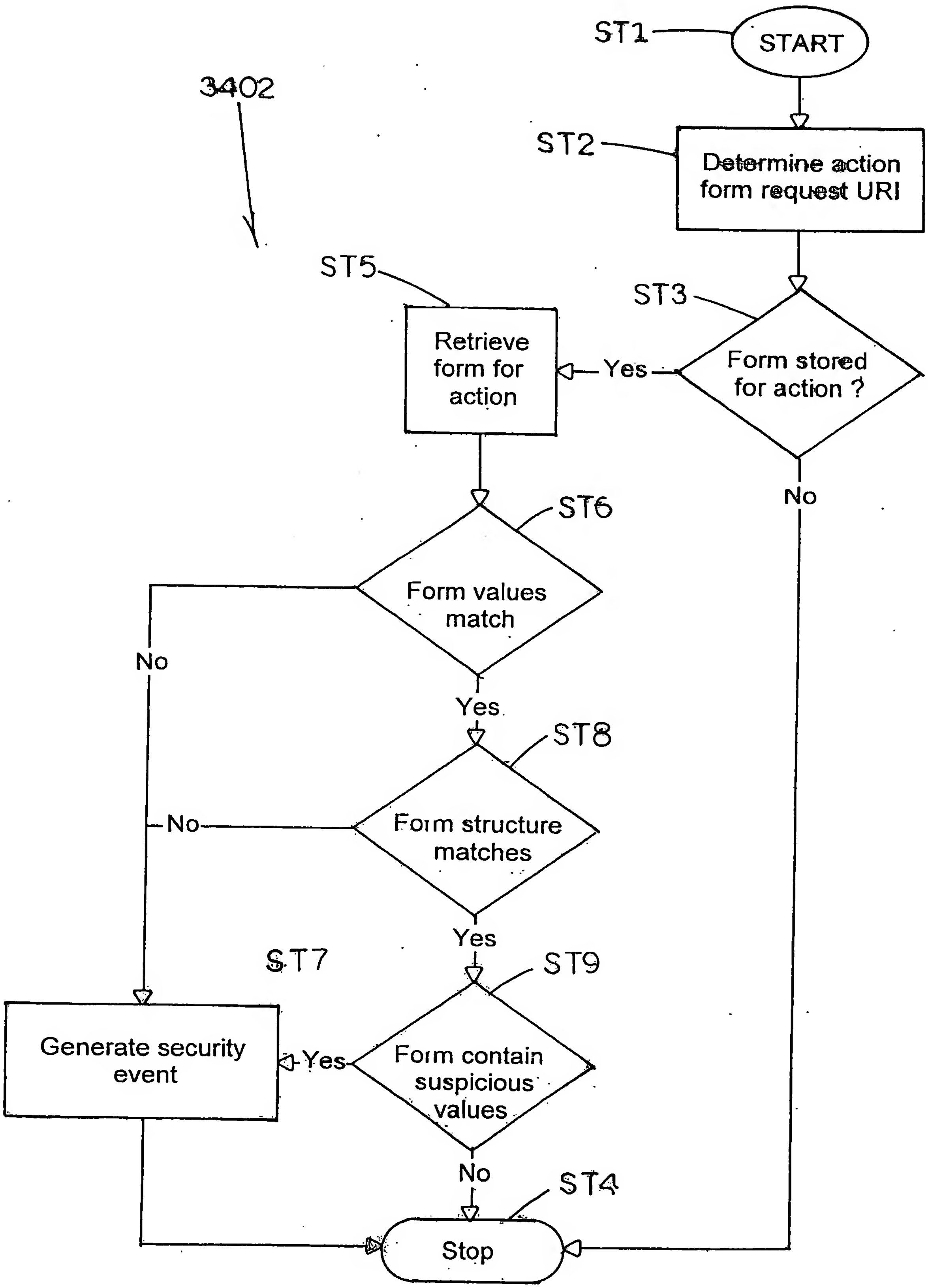


FiG · 34B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

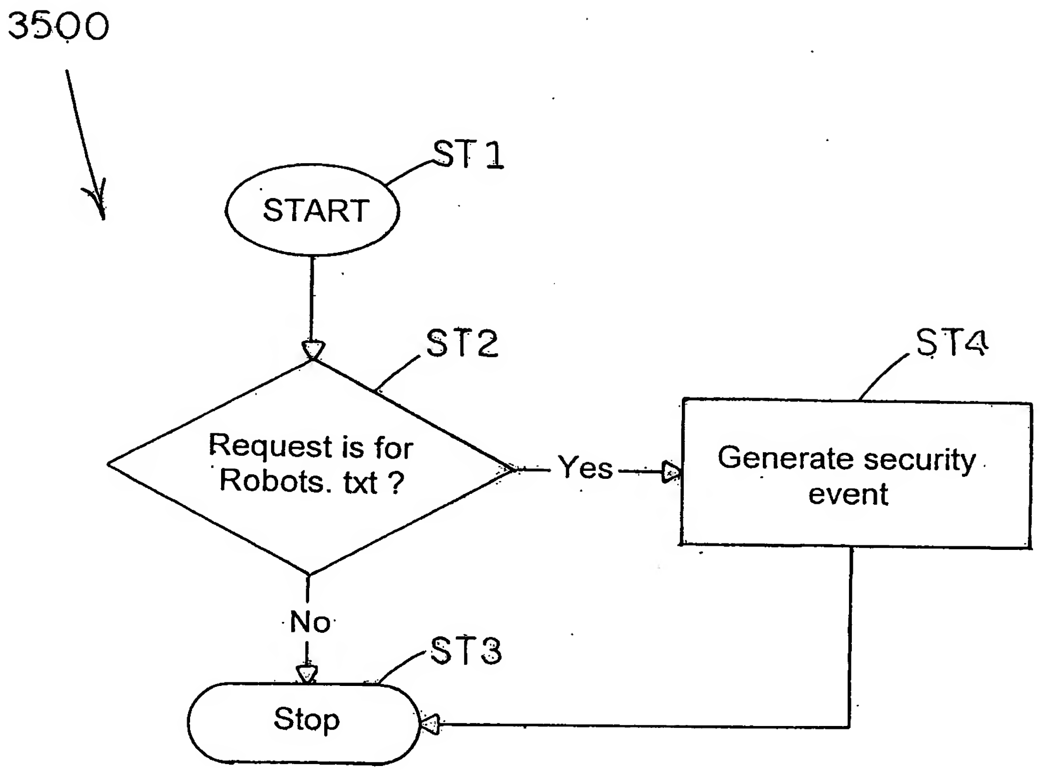


Fig. 35

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

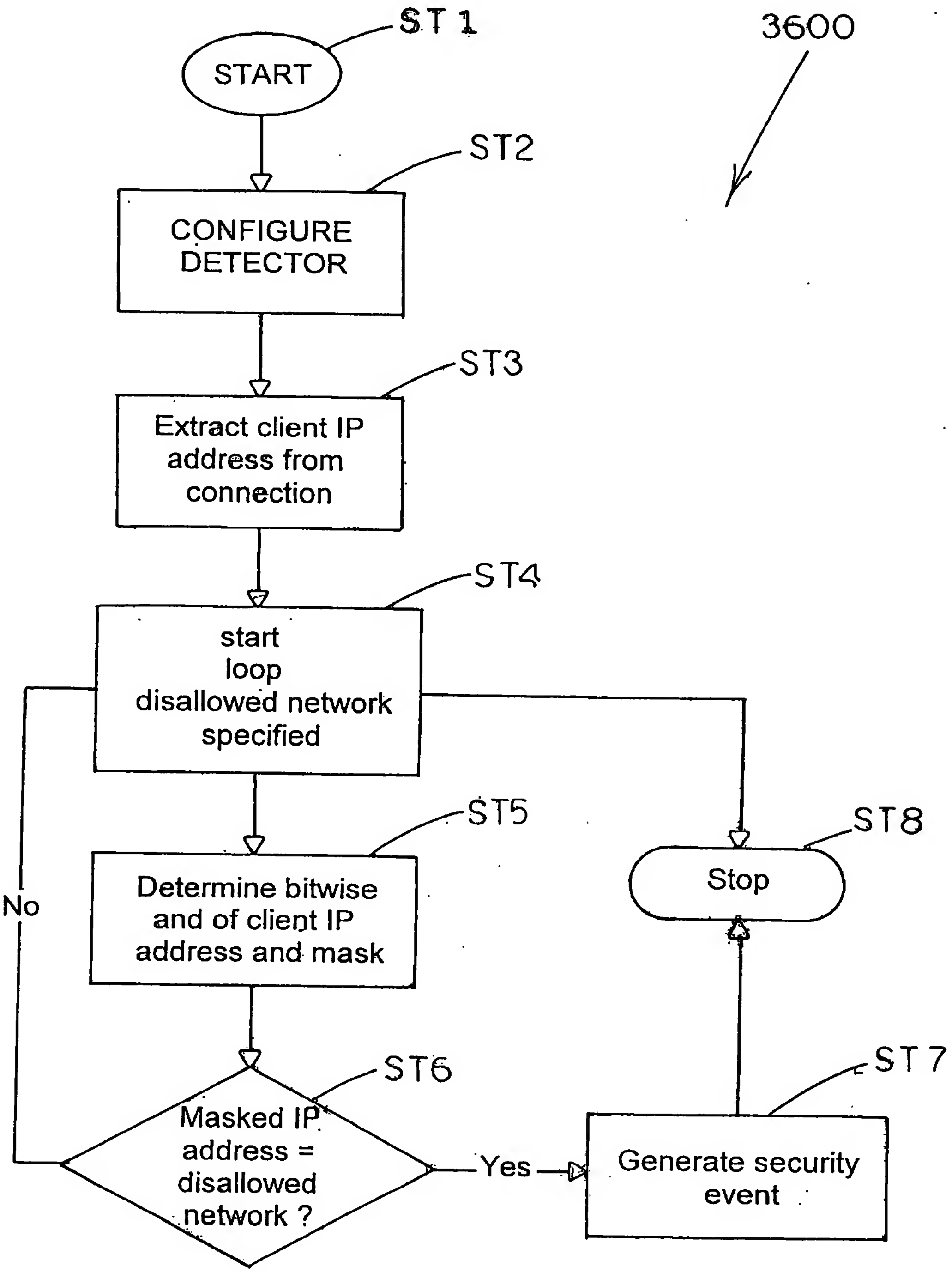

ST 1
3600
START
ST2
CONFIGURE DETECTOR
ST3
Extract client IP address from connection
ST4
start loop disallowed network specified
ST5
Determine bitwise and of client IP address and mask
ST8
Stop
No
ST6
Masked IP address = disallowed network ?
Yes
ST 7
Generate security event

Fig. 36

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

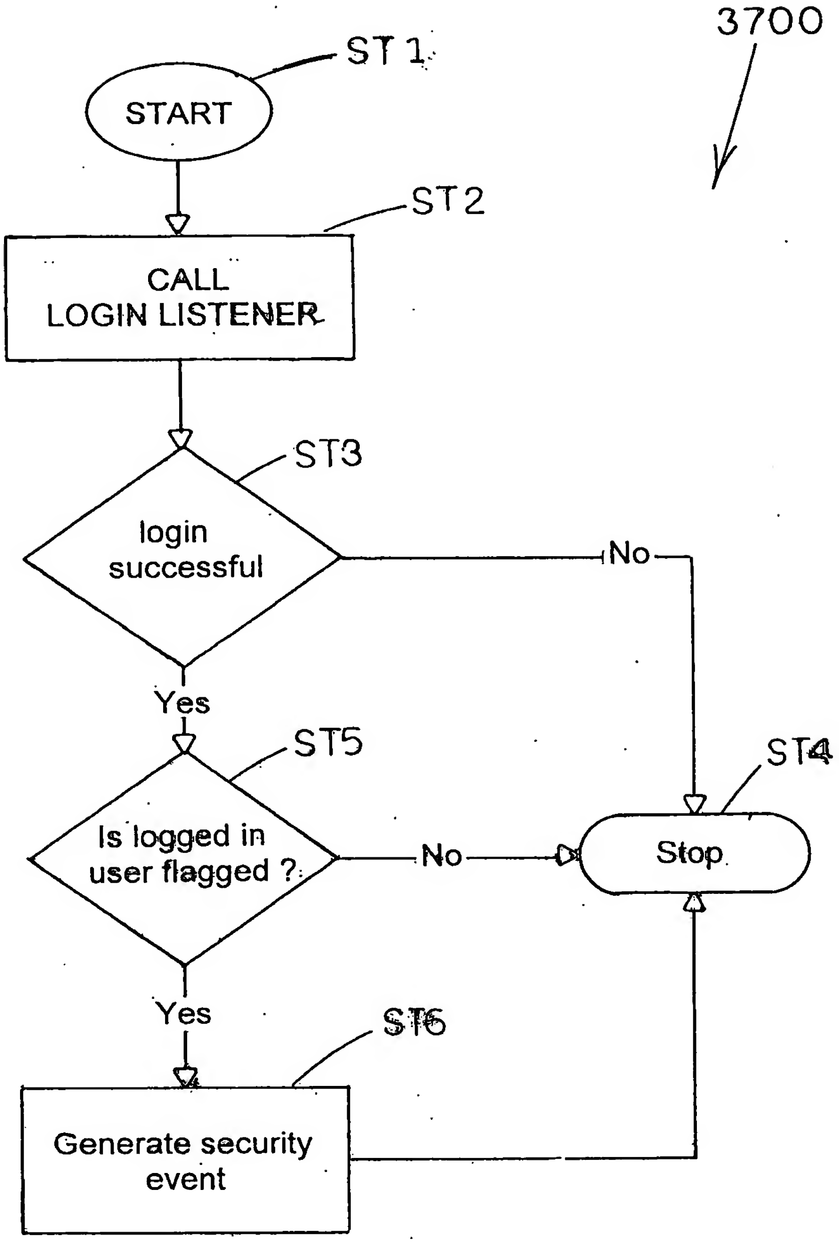


Fig. 37

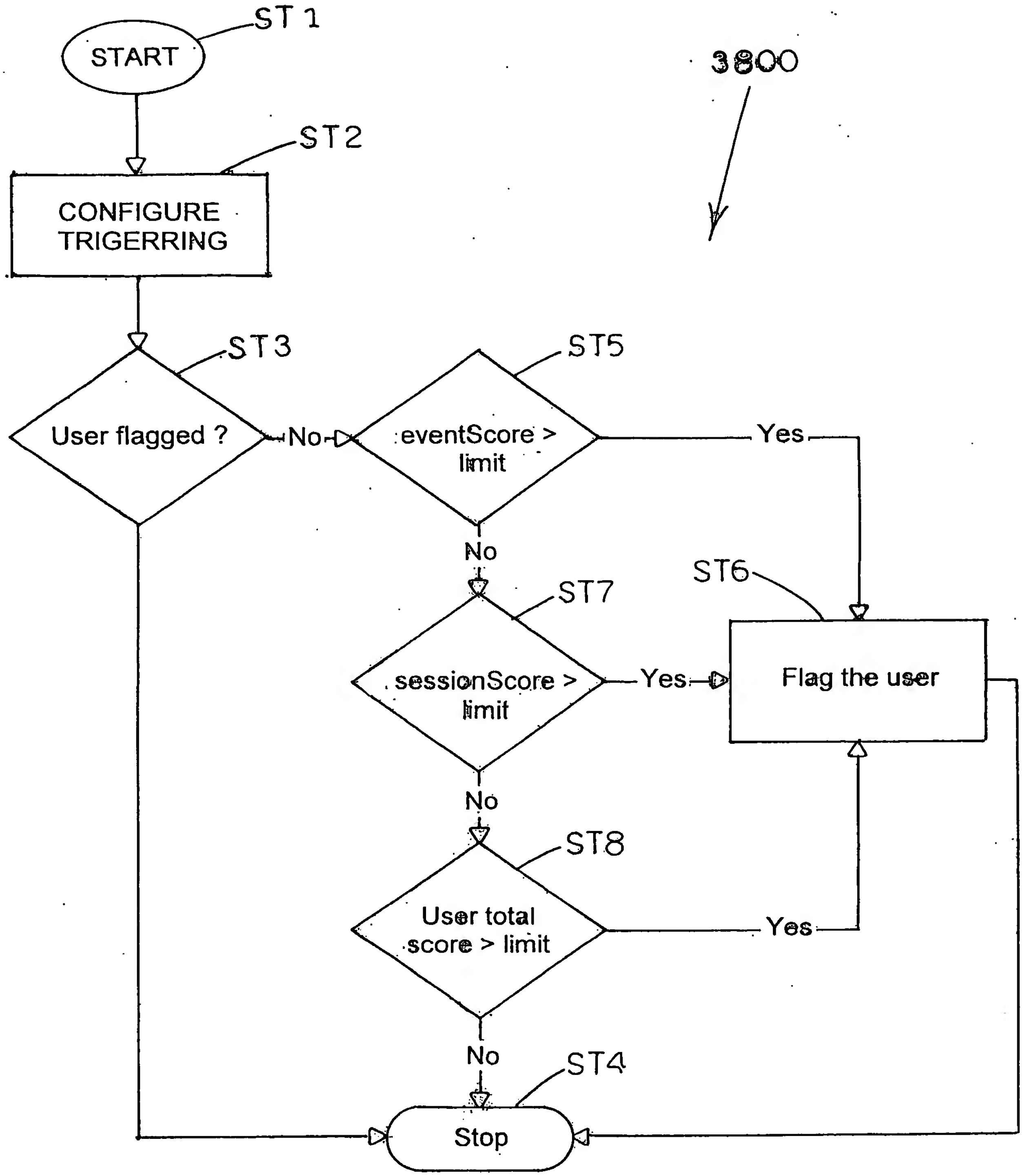
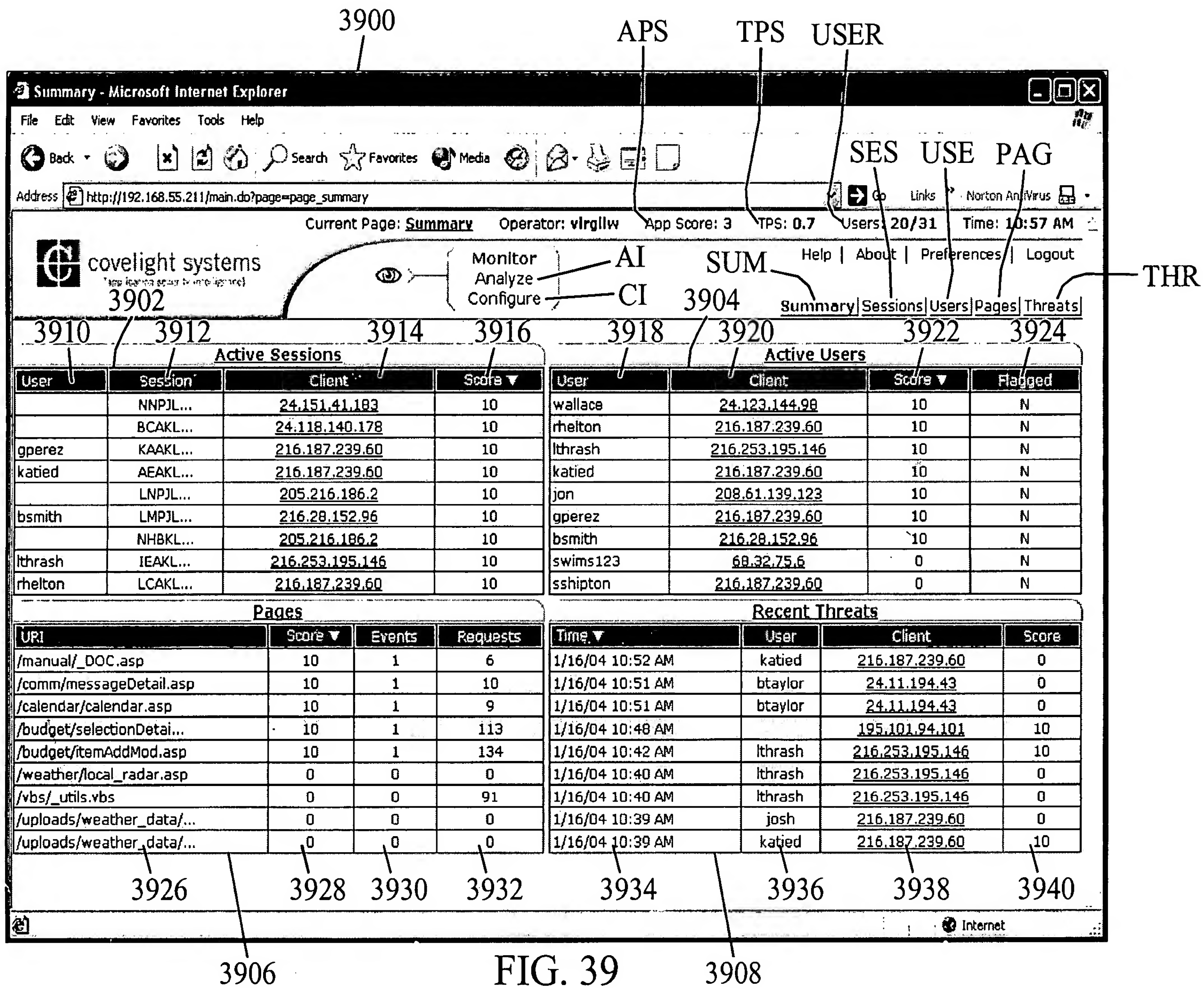

ST 1
START
3800
ST2
CONFIGURE TRIGERRING
ST3
User flagged ?
No
ST5
eventScore > limit
Yes
No
ST6
ST7
sessionScore > limit
Yes
Flag the user
No
ST8
User total score > limit
Yes
No
ST4
Stop

Fig. 38



http://192.168.55.211/main.do?page=page_summary

Current Page: Summary Operator: virgilw App Score: 3 TPS: 0.7 Users: 20/31 Time: 10:57 AM

Active Sessions

User	Session	Client	Score ▼
	NNPJL...	24.151.41.183	10
	BCAKL...	24.118.140.178	10
gperez	KAAKL...	216.187.239.60	10
katied	AEAKL...	216.187.239.60	10
	LNPJL...	205.216.186.2	10
bsmith	LMPJL...	216.28.152.96	10
	NHBKL...	205.216.186.2	10
lthrash	IEAKL...	216.253.195.146	10
rhelton	LCAKL...	216.187.239.60	10

Active Users

User	Client	Score ▼	Flagged
wallace	24.123.144.98	10	N
rhelton	216.187.239.60	10	N
lthrash	216.253.195.146	10	N
katied	216.187.239.60	10	N
jon	208.61.139.123	10	N
gperez	216.187.239.60	10	N
bsmith	216.28.152.96	10	N
swims123	68.32.75.6	0	N
sshipton	216.187.239.60	0	N

Pages

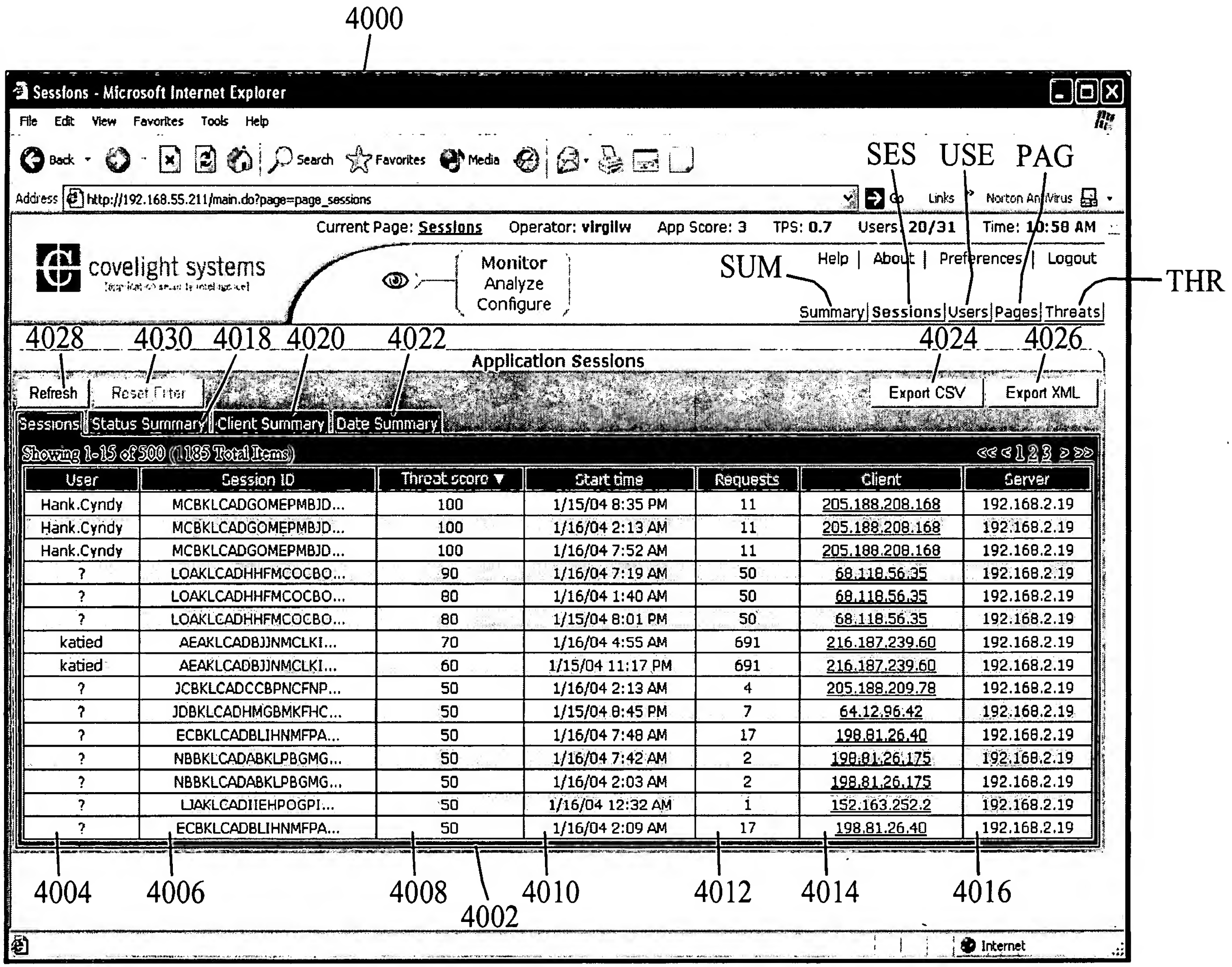
URI	Score ▼	Events	Requests
/manual/_DOC.asp	10	1	6
/comm/messageDetail.asp	10	1	10
/calendar/calendar.asp	10	1	9
/budget/selectionDetai...	10	1	113
/budget/itemAddMod.asp	10	1	134
/weather/local_radar.asp	0	0	0
/vbs/_utils.vbs	0	0	91
/uploads/weather_data/...	0	0	0
/uploads/weather_data/...	0	0	0

Recent Threats

Time ▼	User	Client	Score
1/16/04 10:52 AM	katied	216.187.239.60	0
1/16/04 10:51 AM	btaylor	24.11.194.43	0
1/16/04 10:51 AM	btaylor	24.11.194.43	0
1/16/04 10:48 AM		195.101.94.101	10
1/16/04 10:42 AM	lthrash	216.253.195.146	10
1/16/04 10:40 AM	lthrash	216.253.195.146	0
1/16/04 10:40 AM	lthrash	216.253.195.146	0
1/16/04 10:39 AM	josh	216.187.239.60	0
1/16/04 10:39 AM	katied	216.187.239.60	10

FIG. 39

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

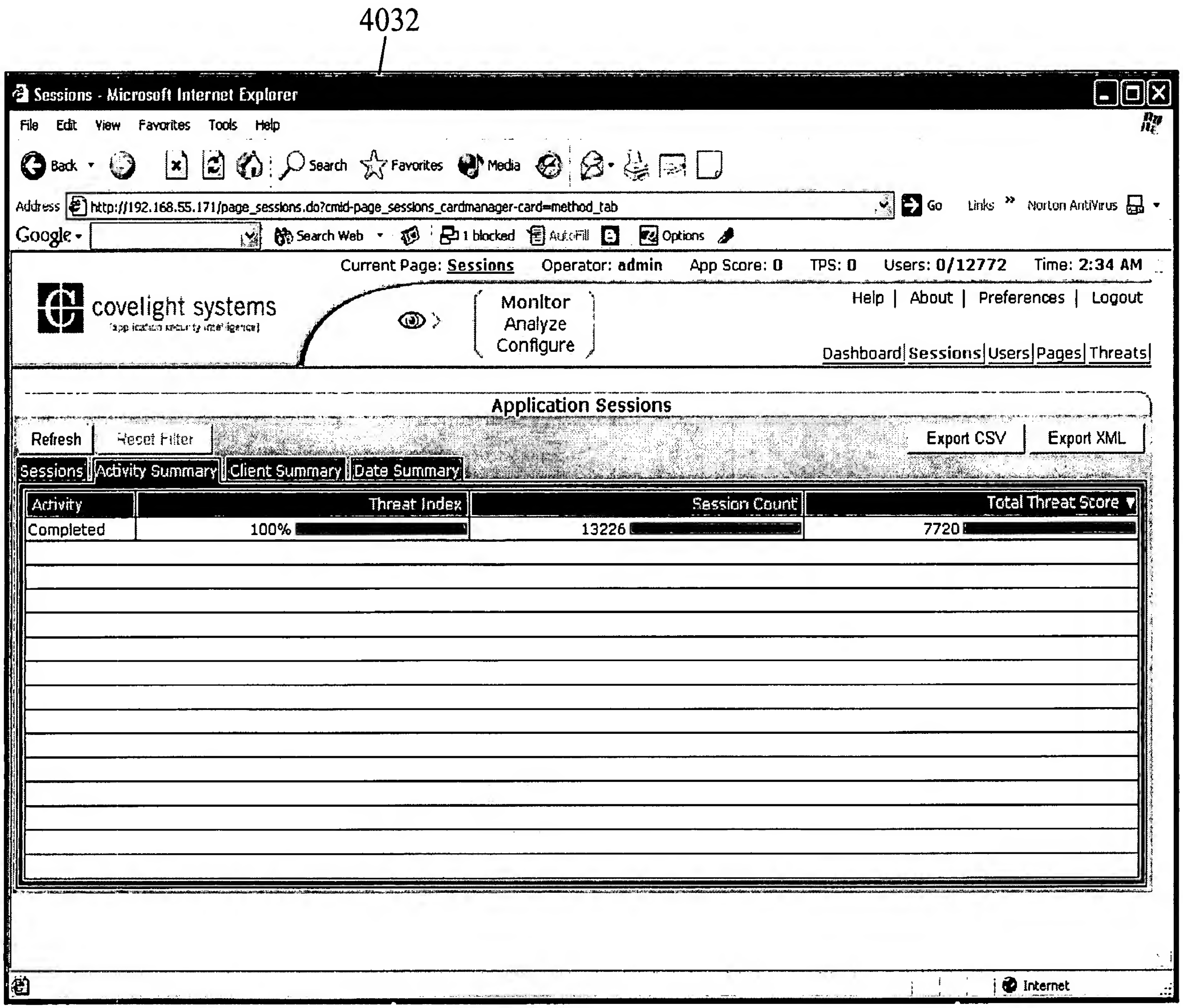

4000
Sessions - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/main.do?page=page_sessions
Go Links Norton AntiVirus
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
SES
USE
PAG
SUM
THR
Summary | Sessions | Users | Pages | Threats
4028
4030
4018
4020
4022
4024
4026
Application Sessions
Refresh
Reset Filter
Export CSV
Export XML
Sessions
Status Summary
Client Summary
Date Summary
<< < 1 2 3 > >>
4004
4006
4008
4002
4010
4012
4014
4016
Internet

Current Page: Sessions Operator: virgilw App Score: 3 TPS: 0.7 Users: 20/31 Time: 10:58 AM

Showing 1-15 of 500 (1185 Total Items)

User	Session ID	Threat score ▼	Start time	Requests	Client	Server
Hank.Cyndy	MCBKLCADGOMEPMBJD...	100	1/15/04 8:35 PM	11	205.188.208.168	192.168.2.19
Hank.Cyndy	MCBKLCADGOMEPMBJD...	100	1/16/04 2:13 AM	11	205.188.208.168	192.168.2.19
Hank.Cyndy	MCBKLCADGOMEPMBJD...	100	1/16/04 7:52 AM	11	205.188.208.168	192.168.2.19
?	LOAKLCADHHFMCOCBO...	90	1/16/04 7:19 AM	50	68.118.56.35	192.168.2.19
?	LOAKLCADHHFMCOCBO...	80	1/16/04 1:40 AM	50	68.118.56.35	192.168.2.19
?	LOAKLCADHHFMCOCBO...	80	1/15/04 8:01 PM	50	68.118.56.35	192.168.2.19
katied	AEAKLCADBJJNMCLKI...	70	1/16/04 4:55 AM	691	216.187.239.60	192.168.2.19
katied	AEAKLCADBJJNMCLKI...	60	1/15/04 11:17 PM	691	216.187.239.60	192.168.2.19
?	JCBKLCADCCBPNCFNP...	50	1/16/04 2:13 AM	4	205.188.209.78	192.168.2.19
?	JDBKLCADHMGBMKFHC...	50	1/15/04 8:45 PM	7	64.12.96.42	192.168.2.19
?	ECBKLCADBLIHNMFPA...	50	1/16/04 7:48 AM	17	198.81.26.40	192.168.2.19
?	NBBKLCADABKLPBGMG...	50	1/16/04 7:42 AM	2	198.81.26.175	192.168.2.19
?	NBBKLCADABKLPBGMG...	50	1/16/04 2:03 AM	2	198.81.26.175	192.168.2.19
?	LJAKLCADIIEHPOGPI...	50	1/16/04 12:32 AM	1	152.163.252.2	192.168.2.19
?	ECBKLCADBLIHNMFPA...	50	1/16/04 2:09 AM	17	198.81.26.40	192.168.2.19

FIG. 40A



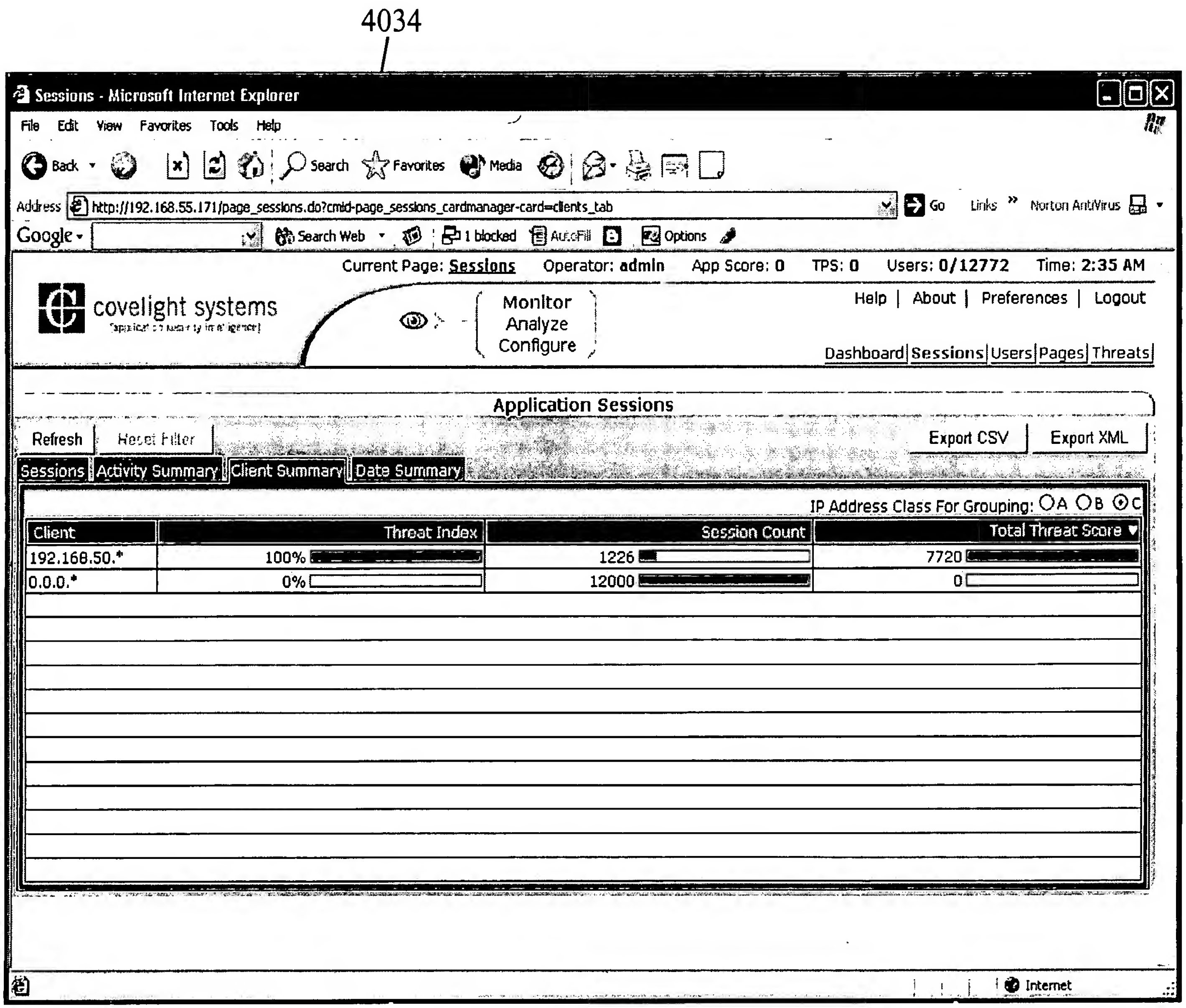
http://192.168.55.171/page_sessions.do?cmd=page_sessions_cardmanager-card=method_tab

Current Page: Sessions Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:34 AM

Application Sessions

Activity	Threat Index	Session Count	Total Threat Score ▼
Completed	100%	13226	7720

FIG. 40B



Address: http://192.168.55.171/page_sessions.do?cmd=page_sessions_cardmanager-card=clients_tab

Current Page: Sessions Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:35 AM

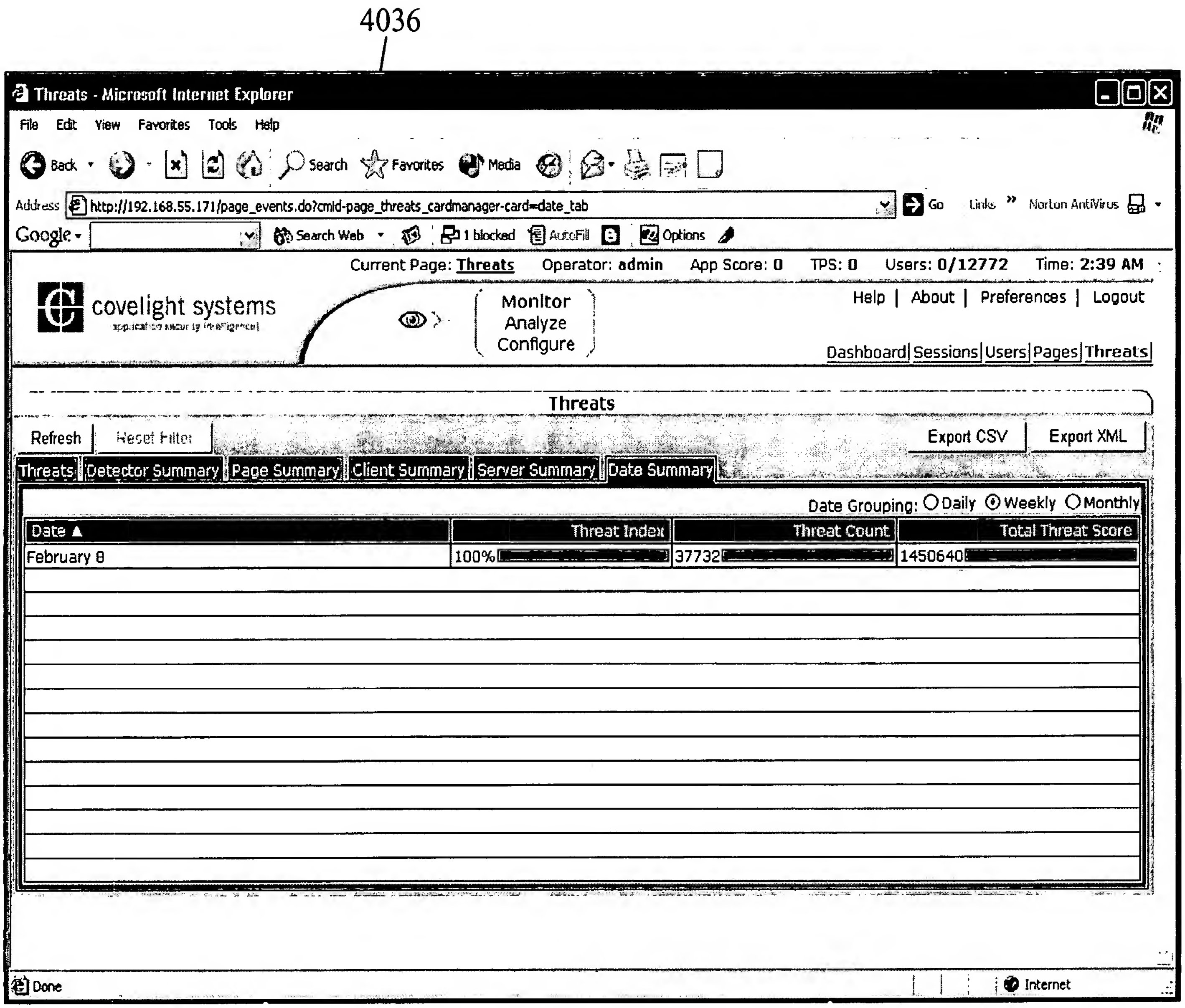
Application Sessions

IP Address Class For Grouping: ○A ○B ●C

Client	Threat Index	Session Count	Total Threat Score ▼
192.168.50.*	100%	1226	7720
0.0.0.*	0%	12000	0

FIG. 40C

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6


4036
Threats - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://192.168.55.171/page_events.do?cmd-page_threats_cardmanager-card=date_tab
Go
Links
Norton AntiVirus
Google
Search Web
1 blocked
AutoFill
Options
covelight systems
application security intelligence
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Dashboard | Sessions | Users | Pages | Threats
Refresh
Reset Filter
Export CSV
Export XML
Threats
Detector Summary
Page Summary
Client Summary
Server Summary
Date Summary
Done
Internet

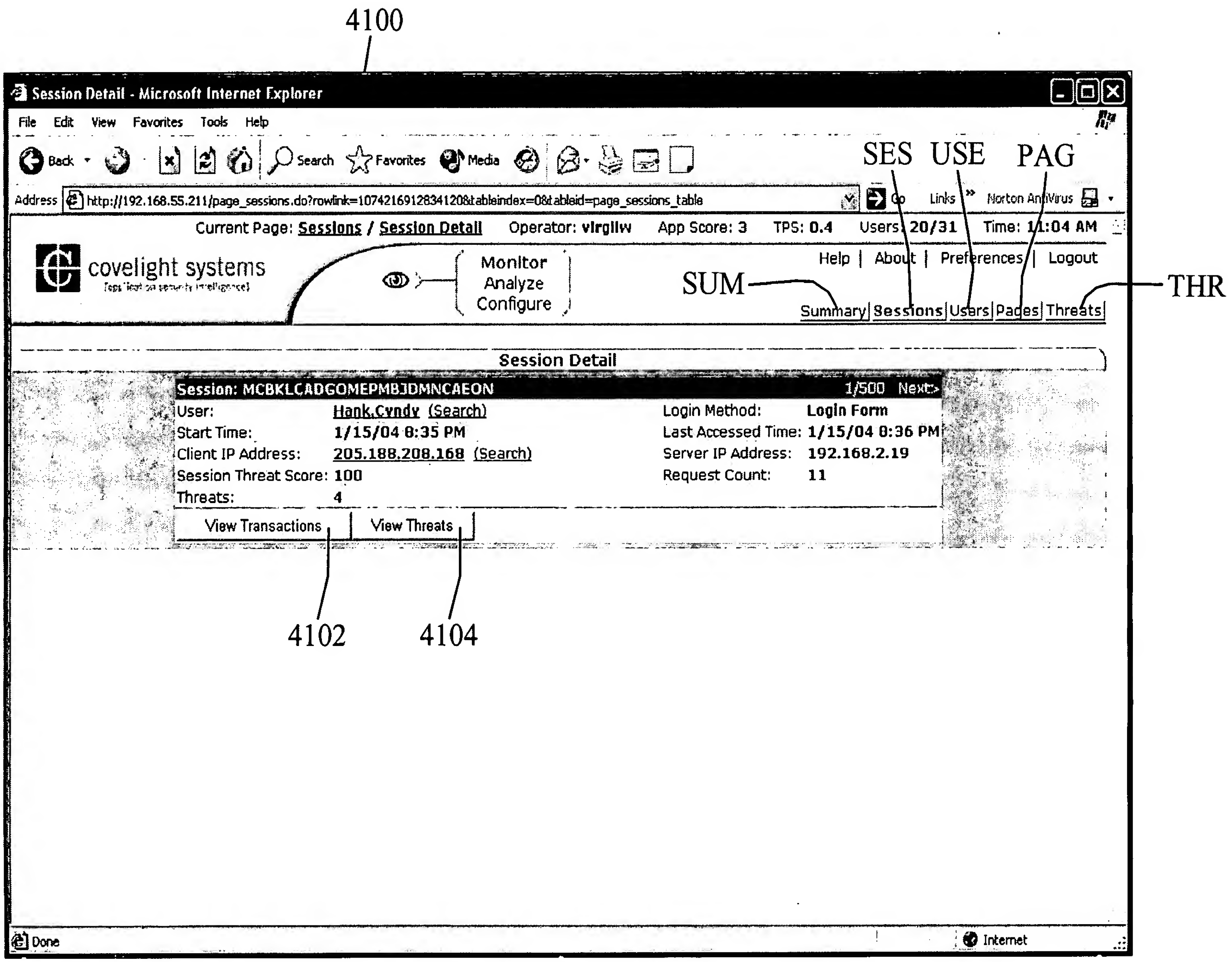
Current Page: Threats Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:39 AM

Threats

Date Grouping: ○ Daily ● Weekly ○ Monthly

Date ▲	Threat Index	Threat Count	Total Threat Score
February 8	100%	37732	1450640

FIG. 40D



http://192.168.55.211/page_sessions.do?rowlink=107421691283412O&tableindex=0&tableid=page_sessions_table

Current Page: Sessions / Session Detail Operator: virgilw App Score: 3 TPS: 0.4 Users: 20/31 Time: 11:04 AM

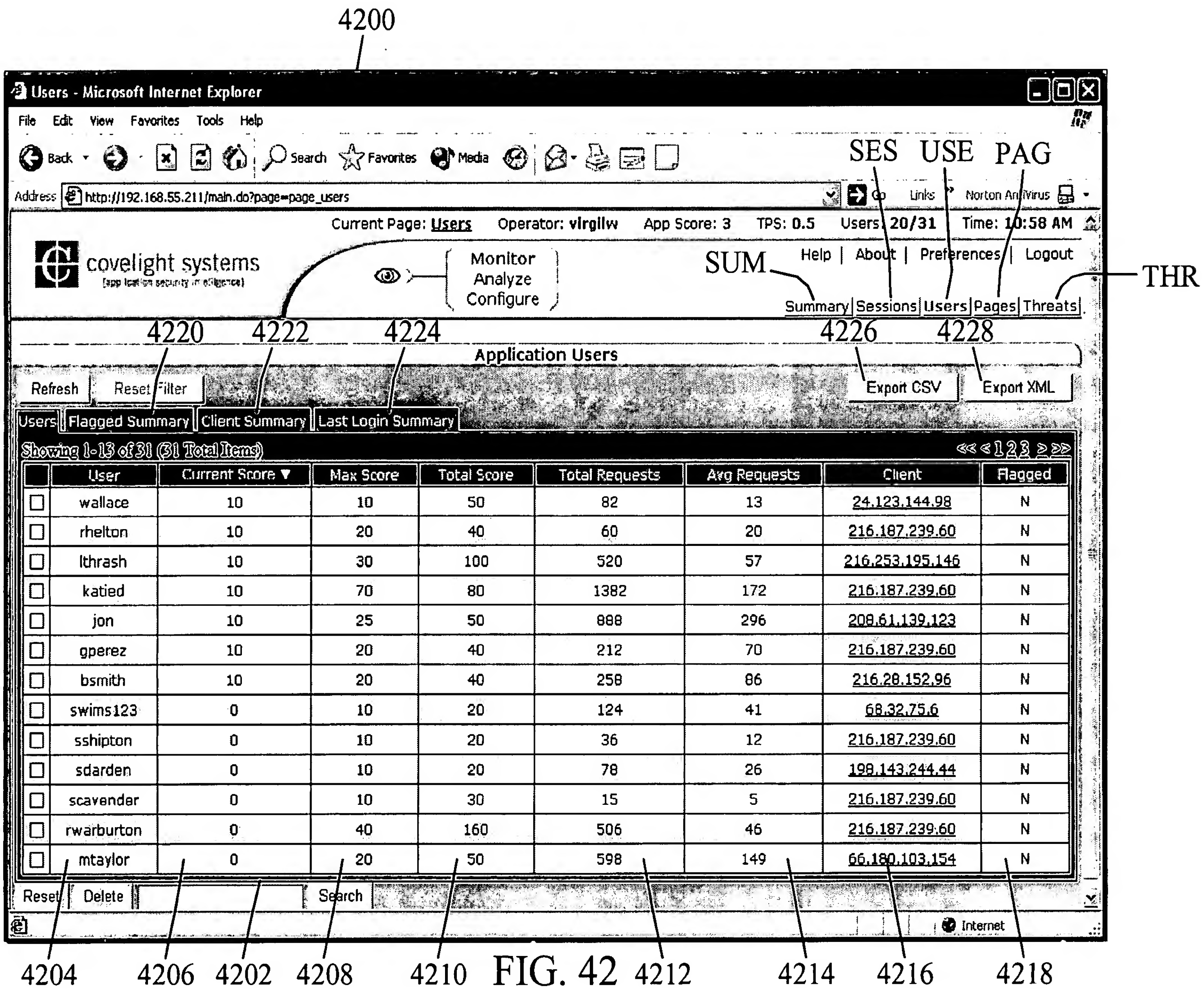
Session Detail

Session: MCBKLCADGOMEPMBJDMNCAEON 1/500 Next>

User:	Hank,Cyndy (Search)	Login Method:	Login Form
Start Time:	1/15/04 8:35 PM	Last Accessed Time:	1/15/04 8:36 PM
Client IP Address:	205.188.208.168 (Search)	Server IP Address:	192.168.2.19
Session Threat Score:	100	Request Count:	11
Threats:	4		

FIG. 41

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6



Current Page: Users Operator: virgilw App Score: 3 TPS: 0.5 Users: 20/31 Time: 10:58 AM

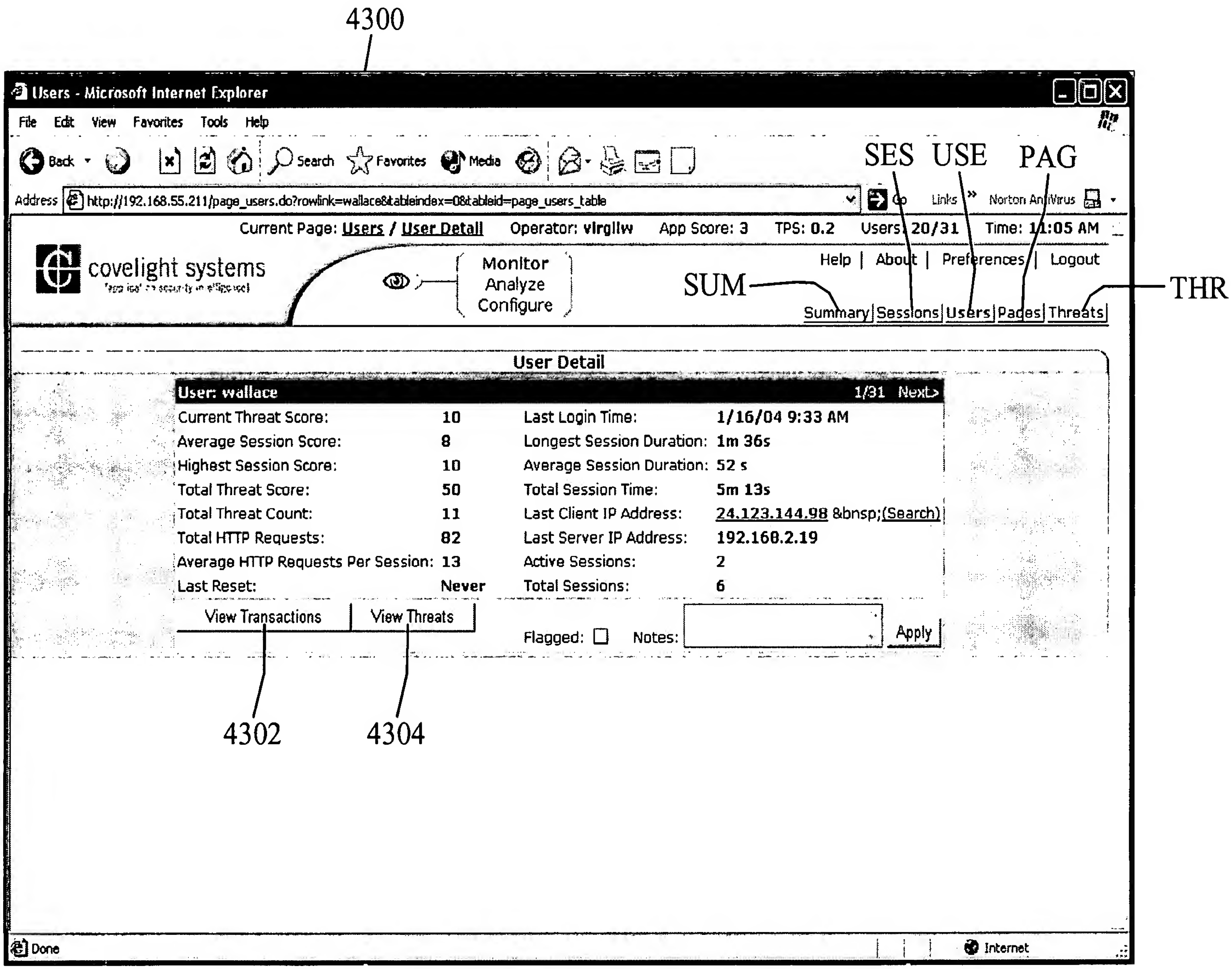
Application Users

Showing 1-13 of 31 (31 Total Items)

	User	Current Score ▼	Max Score	Total Score	Total Requests	Avg Requests	Client	Flagged
□	wallace	10	10	50	82	13	24.123.144.98	N
□	rhelton	10	20	40	60	20	216.187.239.60	N
□	lthrash	10	30	100	520	57	216.253.195.146	N
□	katied	10	70	80	1382	172	216.187.239.60	N
□	jon	10	25	50	888	296	208.61.139.123	N
□	gperez	10	20	40	212	70	216.187.239.60	N
□	bsmith	10	20	40	258	86	216.28.152.96	N
□	swims123	0	10	20	124	41	68.32.75.6	N
□	sshipton	0	10	20	36	12	216.187.239.60	N
□	sdarden	0	10	20	78	26	198.143.244.44	N
□	scavender	0	10	30	15	5	216.187.239.60	N
□	rwarburton	0	40	160	506	46	216.187.239.60	N
□	mtaylor	0	20	50	598	149	66.180.103.154	N

FIG. 42

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6


4300
Users - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_users.do?rowlink=wallace&tableindex=0&tableid=page_users_table
Go Links » Norton AntiVirus
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Summary | Sessions | Users | Pages | Threats
SUM
SES
USE
PAG
THR
View Transactions
View Threats
Apply
Done
Internet
4302
4304

Current Page: Users / User Detail Operator: virgilw App Score: 3 TPS: 0.2 Users: 20/31 Time: 11:05 AM

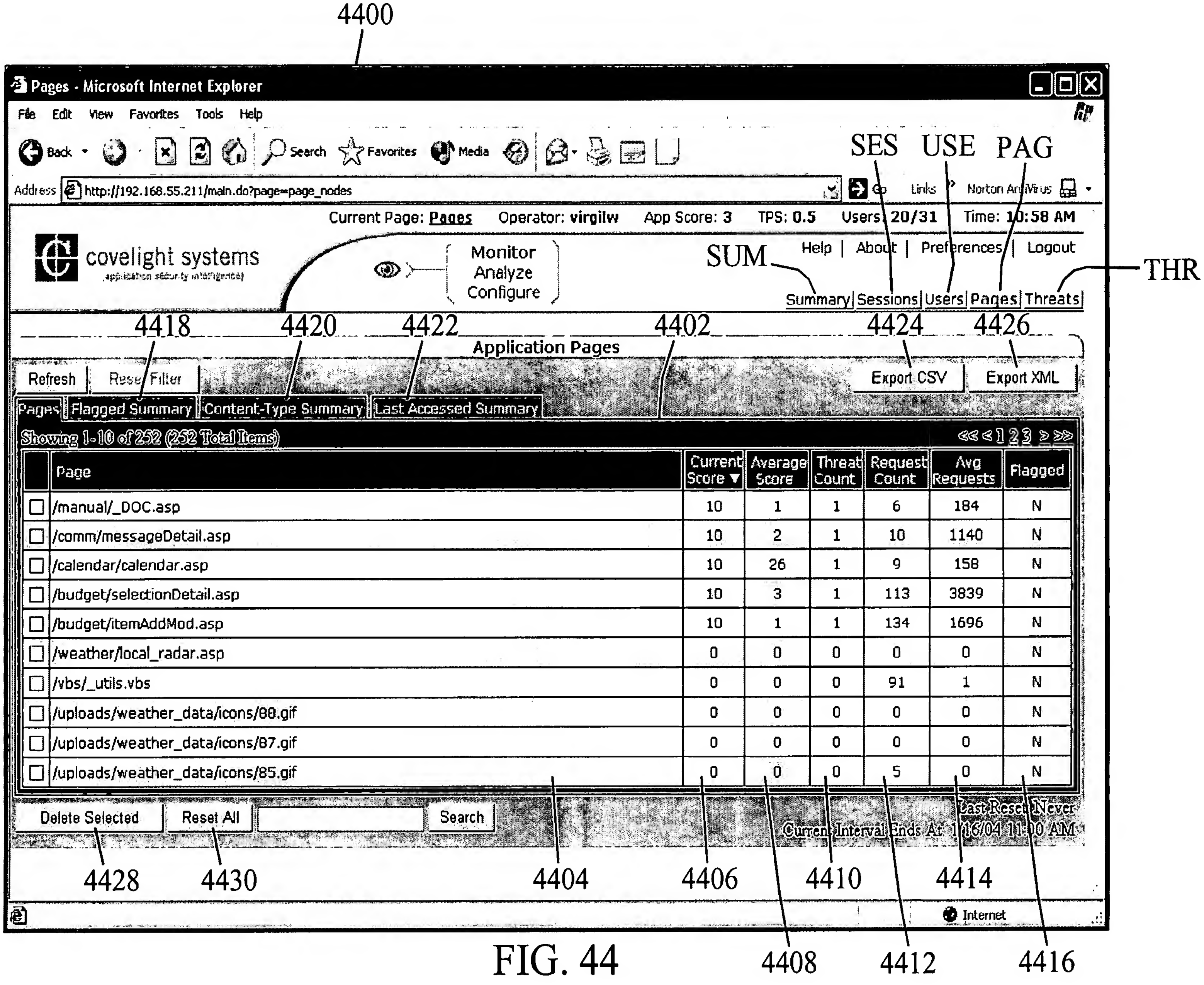
User Detail

User: wallace 1/31 Next>

Current Threat Score:	10	Last Login Time:	1/16/04 9:33 AM
Average Session Score:	8	Longest Session Duration:	1m 36s
Highest Session Score:	10	Average Session Duration:	52 s
Total Threat Score:	50	Total Session Time:	5m 13s
Total Threat Count:	11	Last Client IP Address:	24.123.144.98 &bnsp;(Search)
Total HTTP Requests:	82	Last Server IP Address:	192.168.2.19
Average HTTP Requests Per Session:	13	Active Sessions:	2
Last Reset:	Never	Total Sessions:	6

Flagged: □ Notes:

FIG. 43



http://192.168.55.211/main.do?page=page_nodes

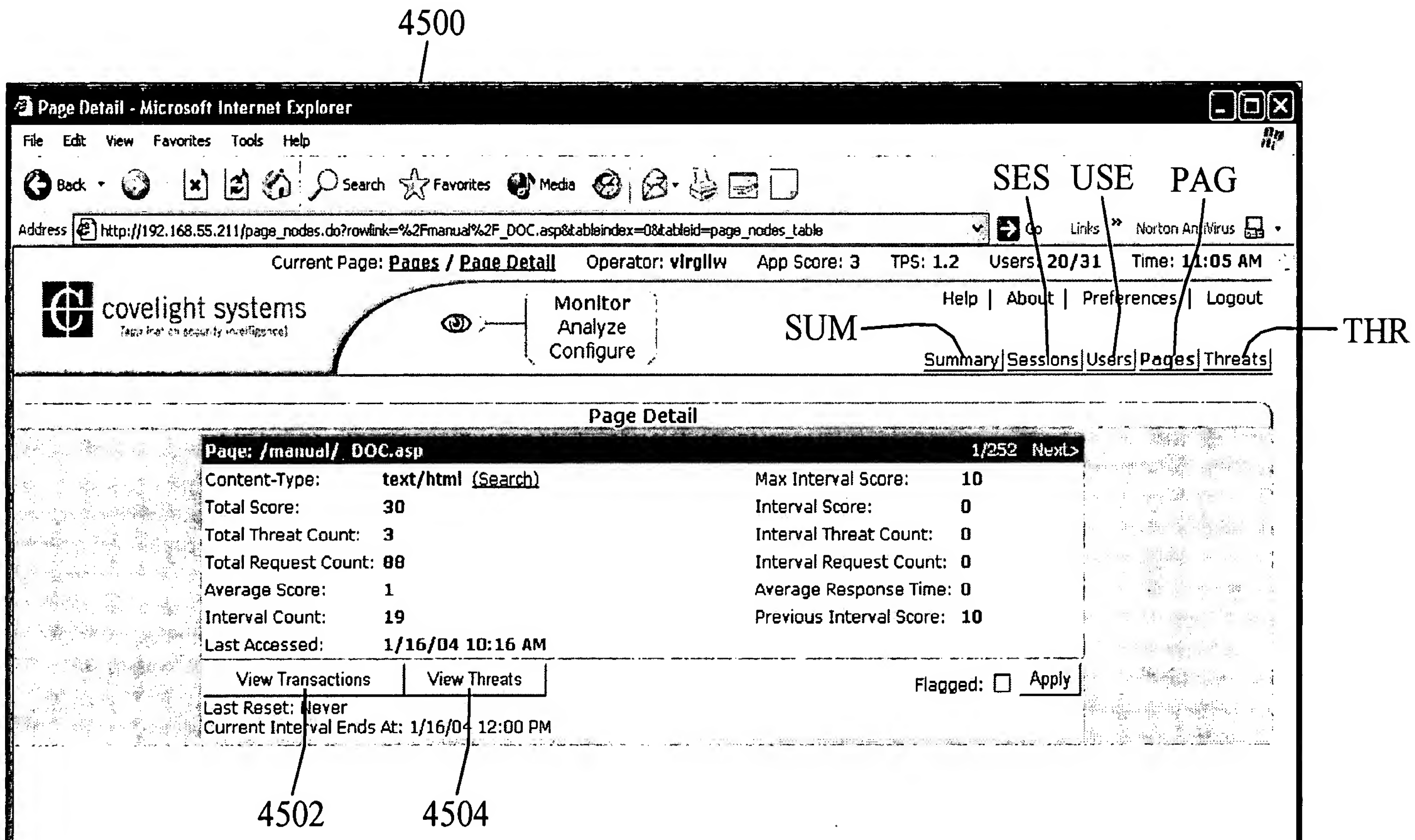
Current Page: Pages Operator: virgilw App Score: 3 TPS: 0.5 Users: 20/31 Time: 10:58 AM

Showing 1-10 of 252 (252 Total Items)

	Page	Current Score ▼	Average Score	Threat Count	Request Count	Avg Requests	Flagged
□	/manual/_DOC.asp	10	1	1	6	184	N
□	/comm/messageDetail.asp	10	2	1	10	1140	N
□	/calendar/calendar.asp	10	26	1	9	158	N
□	/budget/selectionDetail.asp	10	3	1	113	3839	N
□	/budget/itemAddMod.asp	10	1	1	134	1696	N
□	/weather/local_radar.asp	0	0	0	0	0	N
□	/vbs/_utils.vbs	0	0	0	91	1	N
□	/uploads/weather_data/icons/88.gif	0	0	0	0	0	N
□	/uploads/weather_data/icons/87.gif	0	0	0	0	0	N
□	/uploads/weather_data/icons/85.gif	0	0	0	5	0	N

Last Reset: Never
Current Interval Ends At: 1/16/04 11:00 AM

FIG. 44


4500
Page Detail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Links » Norton AntiVirus
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
SUM
SES
USE
PAG
THR
Summary | Sessions | Users | Pages | Threats
View Transactions
View Threats
Apply
4502
4504
Done
Internet

http://192.168.55.211/page_nodes.do?rowlink=%2Fmanual%2F_DOC.asp&tableindex=0&tableid=page_nodes_table

Current Page: Pages / Page Detail   Operator: virgilw   App Score: 3   TPS: 1.2   Users: 20/31   Time: 11:05 AM

Page Detail

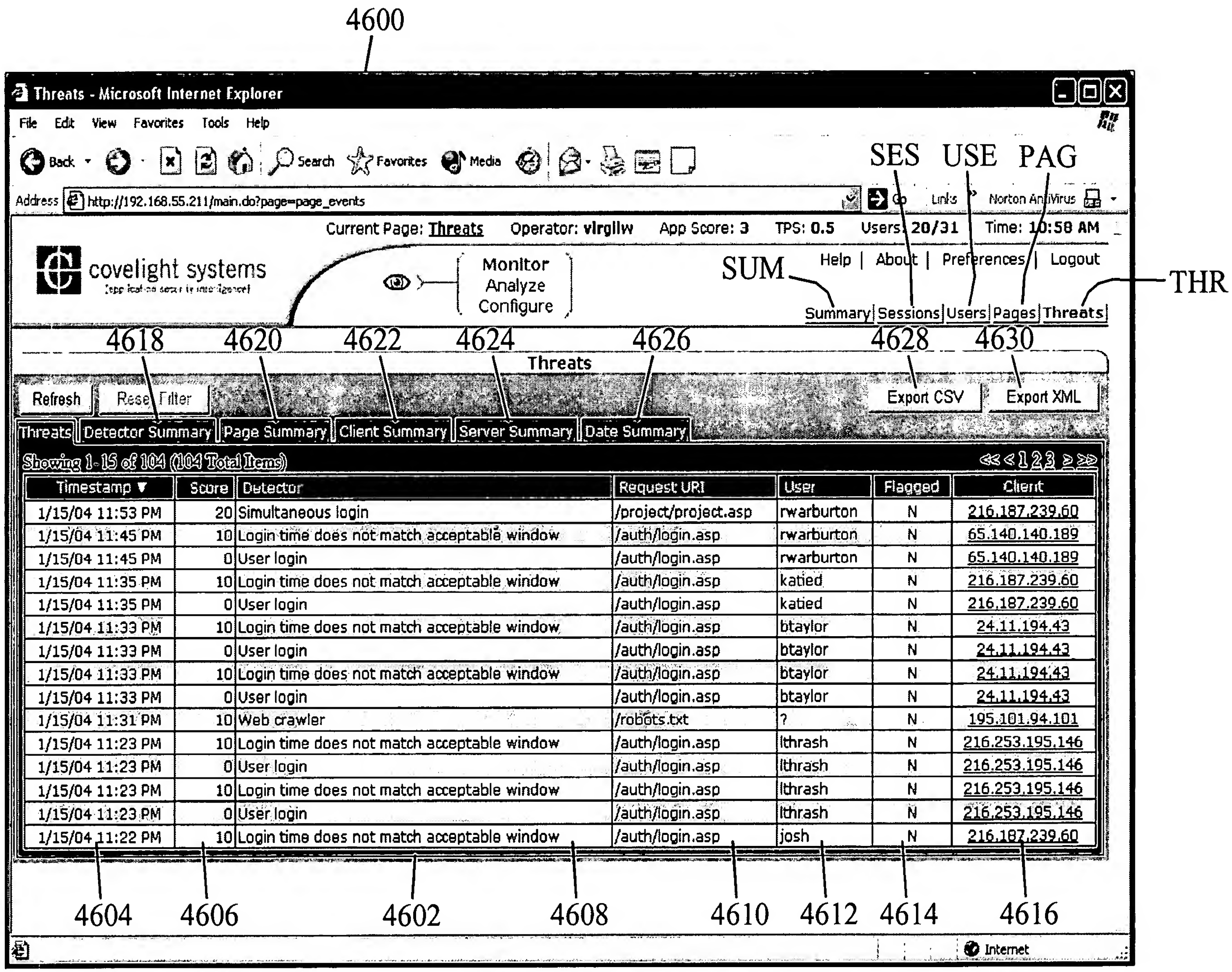
Page: /manual/_DOC.asp   1/252 Next>

Content-Type:	text/html (Search)	Max Interval Score:	10
Total Score:	30	Interval Score:	0
Total Threat Count:	3	Interval Threat Count:	0
Total Request Count:	88	Interval Request Count:	0
Average Score:	1	Average Response Time:	0
Interval Count:	19	Previous Interval Score:	10
Last Accessed:	1/16/04 10:16 AM		

Flagged: □

Last Reset: Never
Current Interval Ends At: 1/16/04 12:00 PM

FIG. 45

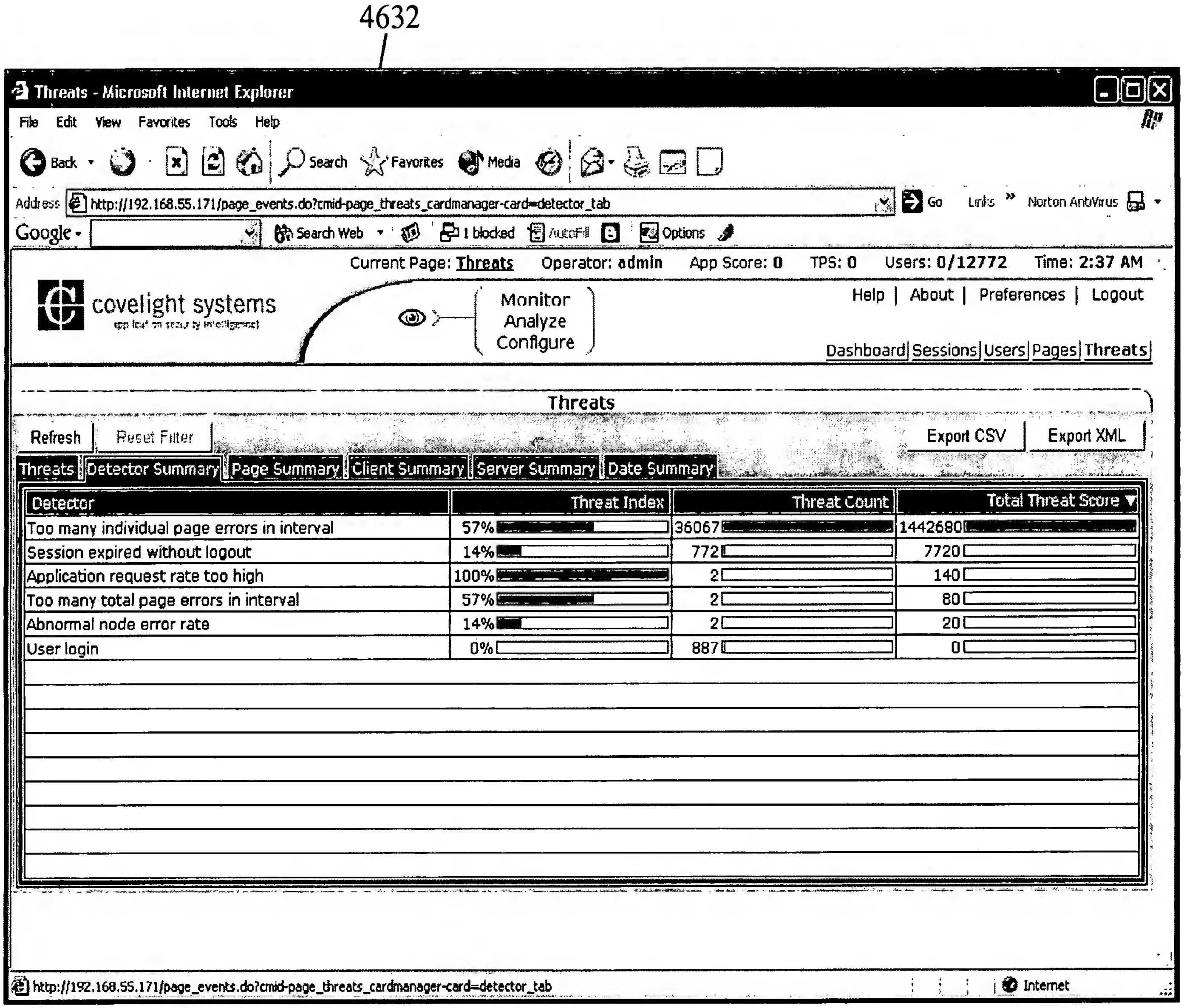

4600
Threats - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/main.do?page=page_events
Go Links Norton AntiVirus
covelight systems
application security intelligence
Monitor
Analyze
Configure
Help | About | Preferences | Logout
SUM
SES
USE
PAG
THR
Summary | Sessions | Users | Pages | Threats
4618
4620
4622
4624
4626
4628
4630
Threats
Refresh
Reset Filter
Export CSV
Export XML
Threats
Detector Summary
Page Summary
Client Summary
Server Summary
Date Summary
<< < 1 2 3 > >>
4604
4606
4602
4608
4610
4612
4614
4616
Internet

Current Page: Threats Operator: virgilw App Score: 3 TPS: 0.5 Users: 20/31 Time: 10:58 AM

Showing 1-15 of 104 (104 Total Items)

Timestamp ▼	Score	Detector	Request URI	User	Flagged	Client
1/15/04 11:53 PM	20	Simultaneous login	/project/project.asp	rwarburton	N	216.187.239.60
1/15/04 11:45 PM	10	Login time does not match acceptable window	/auth/login.asp	rwarburton	N	65.140.140.189
1/15/04 11:45 PM	0	User login	/auth/login.asp	rwarburton	N	65.140.140.189
1/15/04 11:35 PM	10	Login time does not match acceptable window	/auth/login.asp	katied	N	216.187.239.60
1/15/04 11:35 PM	0	User login	/auth/login.asp	katied	N	216.187.239.60
1/15/04 11:33 PM	10	Login time does not match acceptable window	/auth/login.asp	btaylor	N	24.11.194.43
1/15/04 11:33 PM	0	User login	/auth/login.asp	btaylor	N	24.11.194.43
1/15/04 11:33 PM	10	Login time does not match acceptable window	/auth/login.asp	btaylor	N	24.11.194.43
1/15/04 11:33 PM	0	User login	/auth/login.asp	btaylor	N	24.11.194.43
1/15/04 11:31 PM	10	Web crawler	/robots.txt	?	N	195.101.94.101
1/15/04 11:23 PM	10	Login time does not match acceptable window	/auth/login.asp	lthrash	N	216.253.195.146
1/15/04 11:23 PM	0	User login	/auth/login.asp	lthrash	N	216.253.195.146
1/15/04 11:23 PM	10	Login time does not match acceptable window	/auth/login.asp	lthrash	N	216.253.195.146
1/15/04 11:23 PM	0	User login	/auth/login.asp	lthrash	N	216.253.195.146
1/15/04 11:22 PM	10	Login time does not match acceptable window	/auth/login.asp	josh	N	216.187.239.60

FIG. 46A


4632
Threats - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.171/page_events.do?cmid-page_threats_cardmanager-card=detector_tab
Go Links » Norton AntiVirus
Google - Search Web 1 blocked AutoFill Options
covelight systems
app lcation security intelligence
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Dashboard | Sessions | Users | Pages | Threats
Refresh
Reset Filter
Export CSV
Export XML
Threats
Detector Summary
Page Summary
Client Summary
Server Summary
Date Summary
http://192.168.55.171/page_events.do?cmid-page_threats_cardmanager-card=detector_tab
Internet

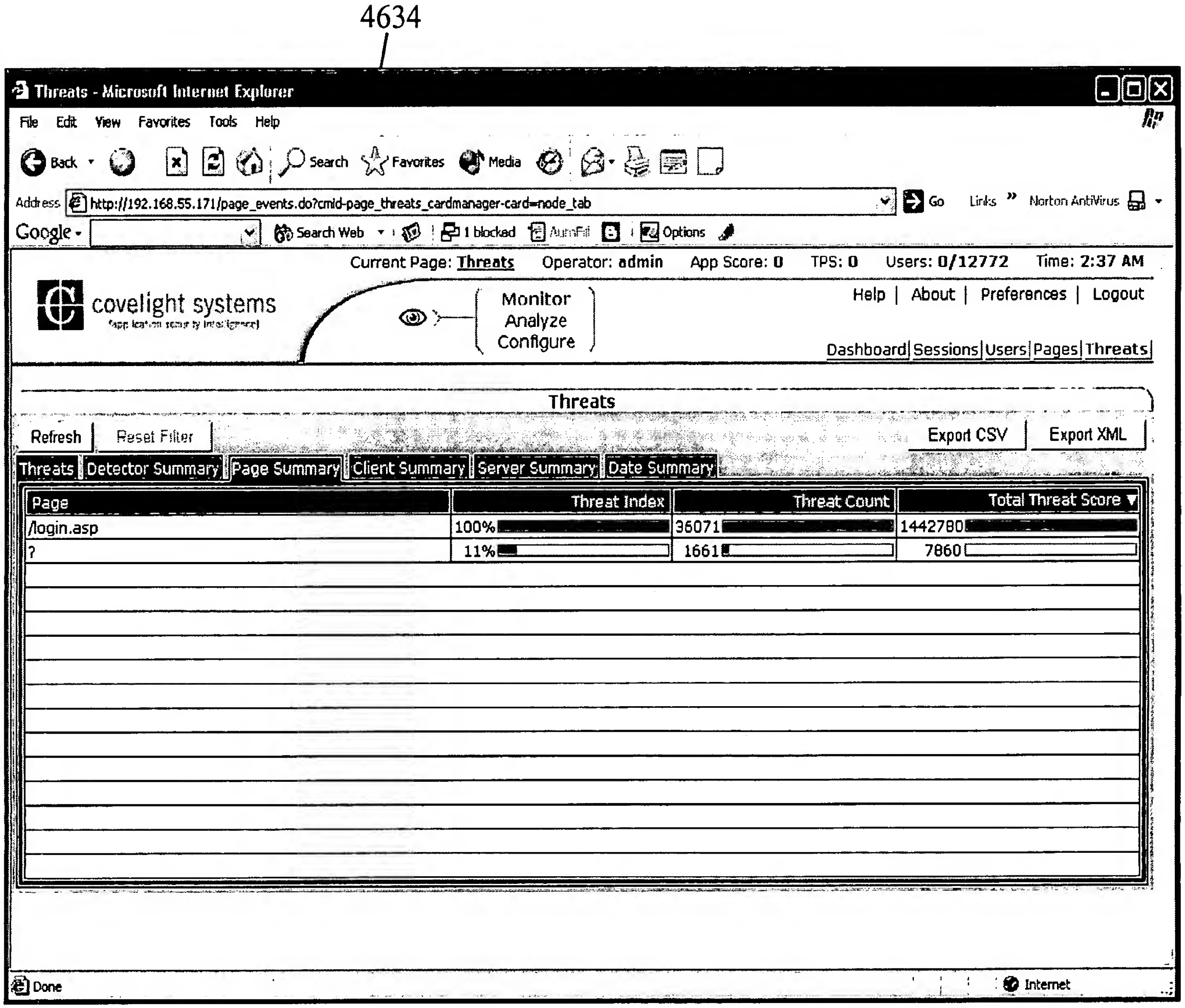
Current Page: Threats Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:37 AM

Threats

Detector	Threat Index	Threat Count	Total Threat Score ▼
Too many individual page errors in interval	57%	36067	1442680
Session expired without logout	14%	772	7720
Application request rate too high	100%	2	140
Too many total page errors in interval	57%	2	80
Abnormal node error rate	14%	2	20
User login	0%	887	0

FIG. 46B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6



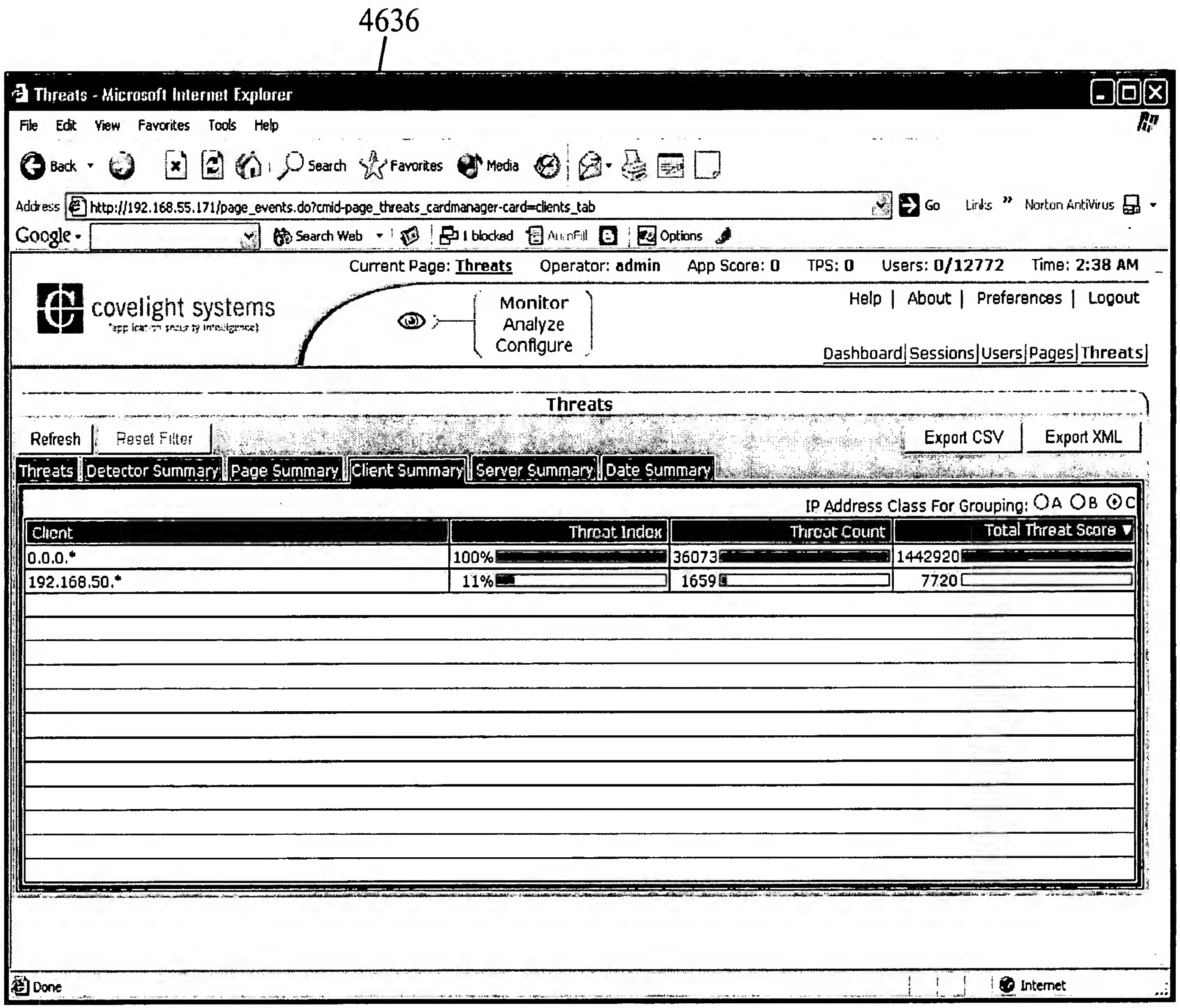
http://192.168.55.171/page_events.do?cmd=page_threats_cardmanager-card=node_tab

Current Page: Threats Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:37 AM

Threats

Page	Threat Index	Threat Count	Total Threat Score ▼
/login.asp	100%	36071	1442780
?	11%	1661	7860

FIG. 46C


4636
Threats - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links » Norton AntiVirus
Google Search Web 1 blocked AutoFill Options
covelight systems
"application security intelligence"
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Dashboard | Sessions | Users | Pages | Threats
Refresh
Reset Filter
Export CSV
Export XML
Threats
Detector Summary
Page Summary
Client Summary
Server Summary
Date Summary
Done
Internet

http://192.168.55.171/page_events.do?cmid-page_threats_cardmanager-card=clients_tab

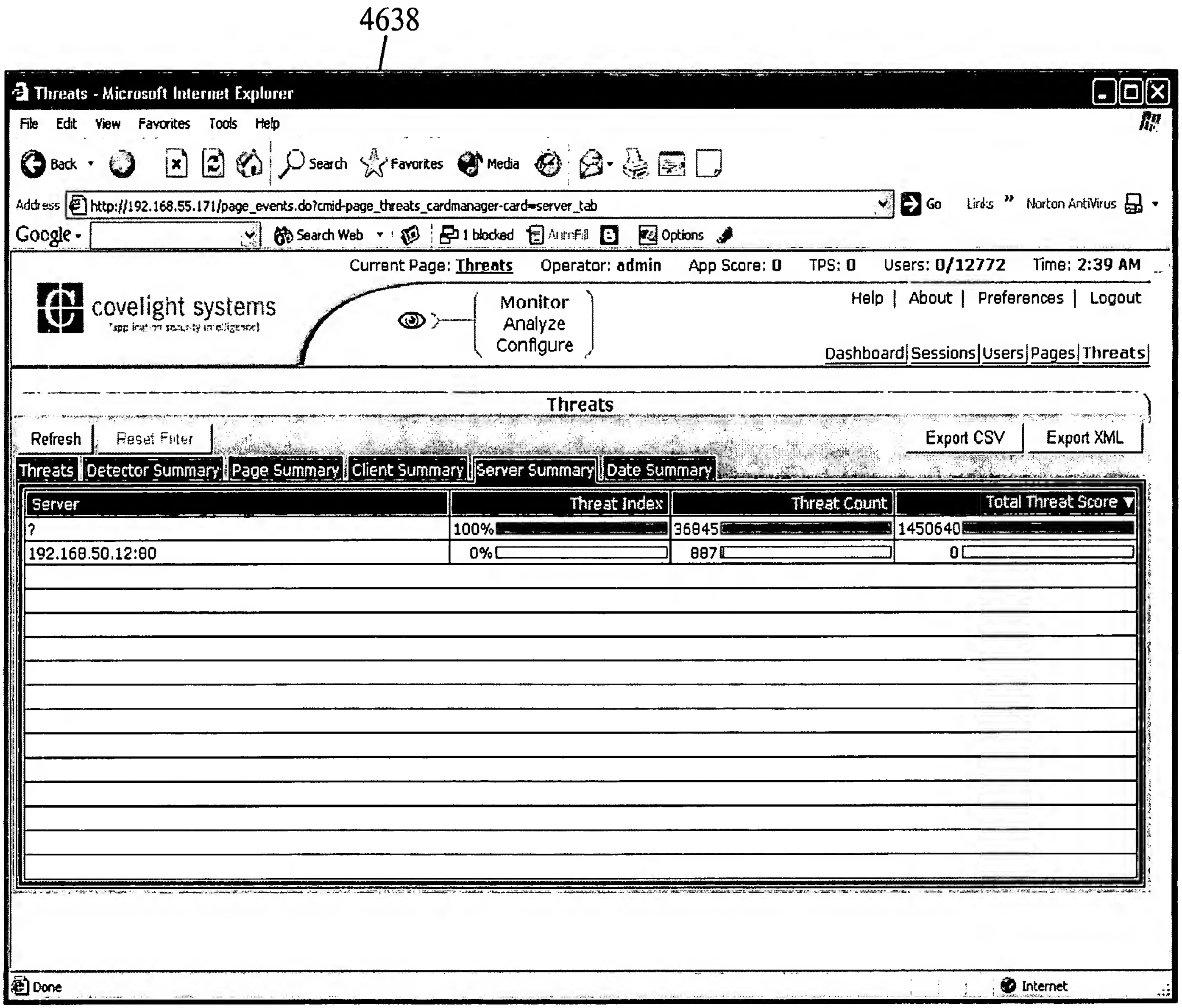
Current Page: Threats Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:38 AM

Threats

IP Address Class For Grouping: ○A ○B ⦿C

Client	Threat Index	Threat Count	Total Threat Score ▼
0.0.0.*	100%	36073	1442920
192.168.50.*	11%	1659	7720

FIG. 46D

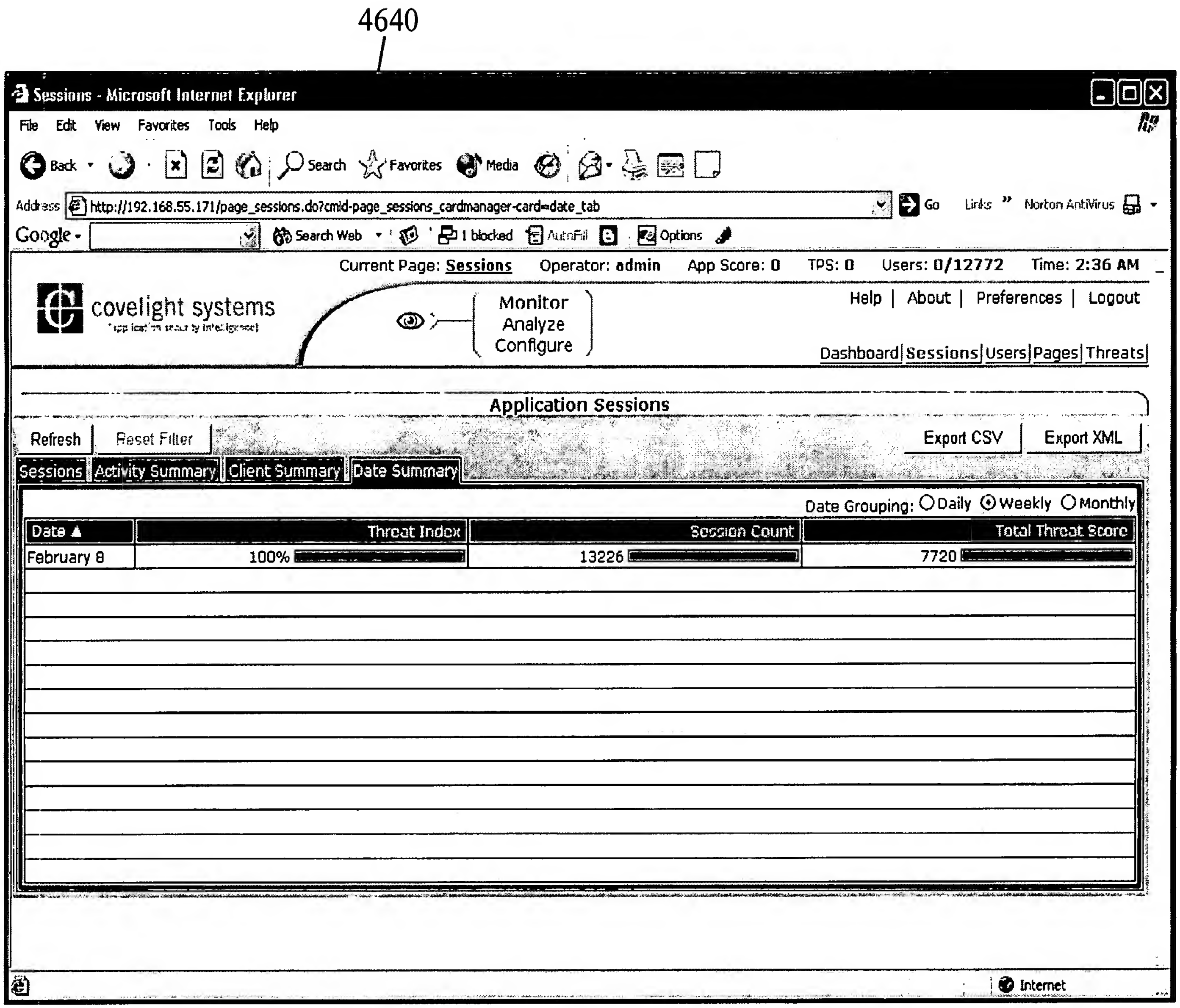

4638
Threats - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.171/page_events.do?cmd=page_threats_cardmanager-card=server_tab
Go Links Norton AntiVirus
Google Search Web 1 blocked AutoFill Options
covelight systems
application security intelligence
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Dashboard | Sessions | Users | Pages | Threats
Refresh
Reset Filter
Export CSV
Export XML
Threats
Detector Summary
Page Summary
Client Summary
Server Summary
Date Summary
Done
Internet

Current Page: Threats Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:39 AM

Threats

Server	Threat Index	Threat Count	Total Threat Score ▼
?	100%	36845	1450640
192.168.50.12:80	0%	887	0

FIG. 46E



Address: http://192.168.55.171/page_sessions.do?cmd=page_sessions_cardmanager-card=date_tab

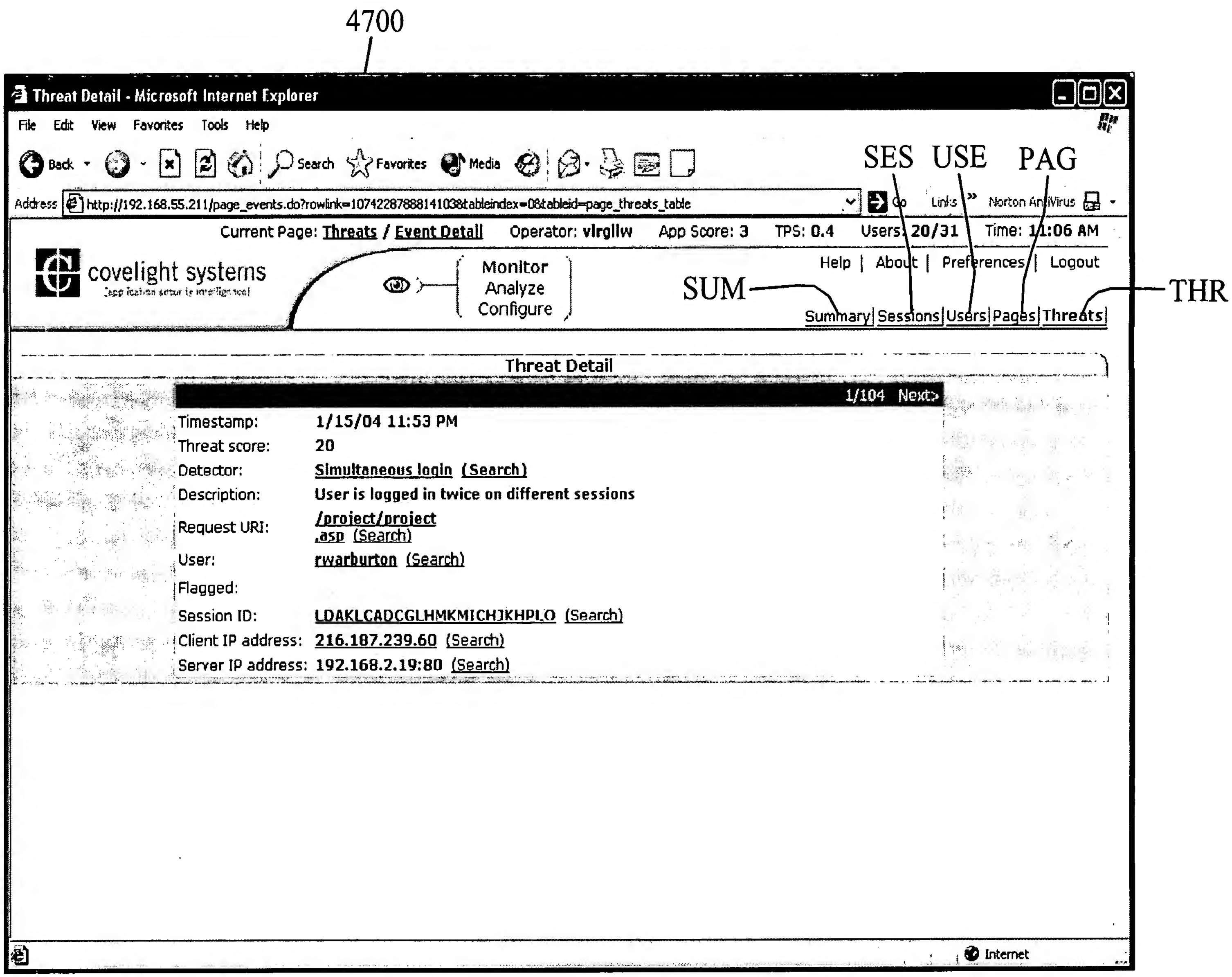
Current Page: Sessions Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:36 AM

Application Sessions

Date Grouping: ○ Daily ● Weekly ○ Monthly

Date ▲	Threat Index	Session Count	Total Threat Score
February 8	100%	13226	7720

FIG. 46F


4700
Threat Detail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links Norton AntiVirus
covelight systems
application security intelligence
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Summary | Sessions | Users | Pages | Threats
SUM
SES
USE
PAG
THR
Internet

Address http://192.168.55.211/page_events.do?rowlink=10742287888141038tableindex=0&tableid=page_threats_table

Current Page: Threats / Event Detail Operator: virgilw App Score: 3 TPS: 0.4 Users: 20/31 Time: 11:06 AM

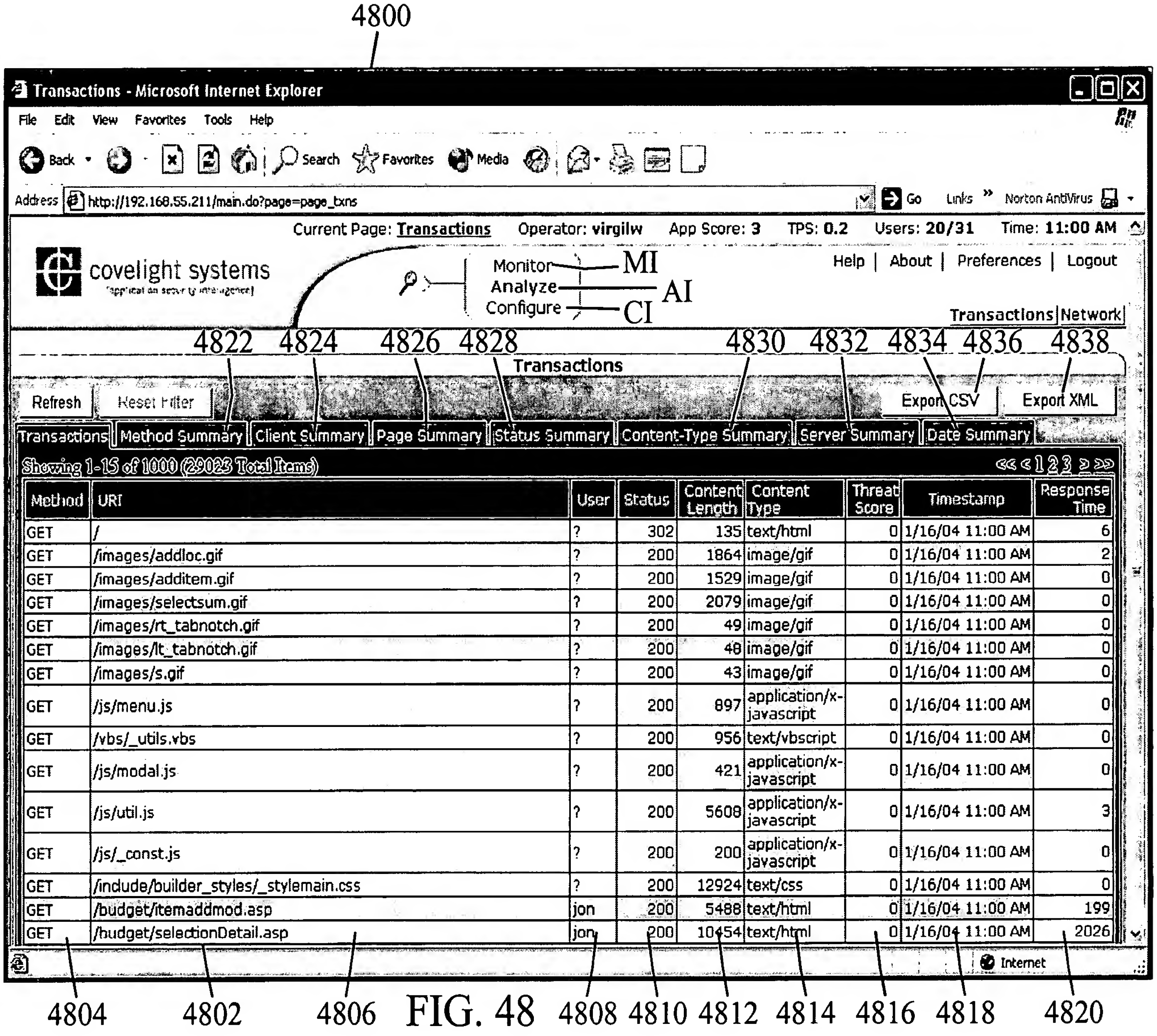
Threat Detail

1/104 Next>

Timestamp:	1/15/04 11:53 PM
Threat score:	20
Detector:	Simultaneous login (Search)
Description:	User is logged in twice on different sessions
Request URI:	/project/project .asp (Search)
User:	rwarburton (Search)
Flagged:	
Session ID:	LDAKLCADCGLHMKMICHJKHPLO (Search)
Client IP address:	216.187.239.60 (Search)
Server IP address:	192.168.2.19:80 (Search)

FIG. 47

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6



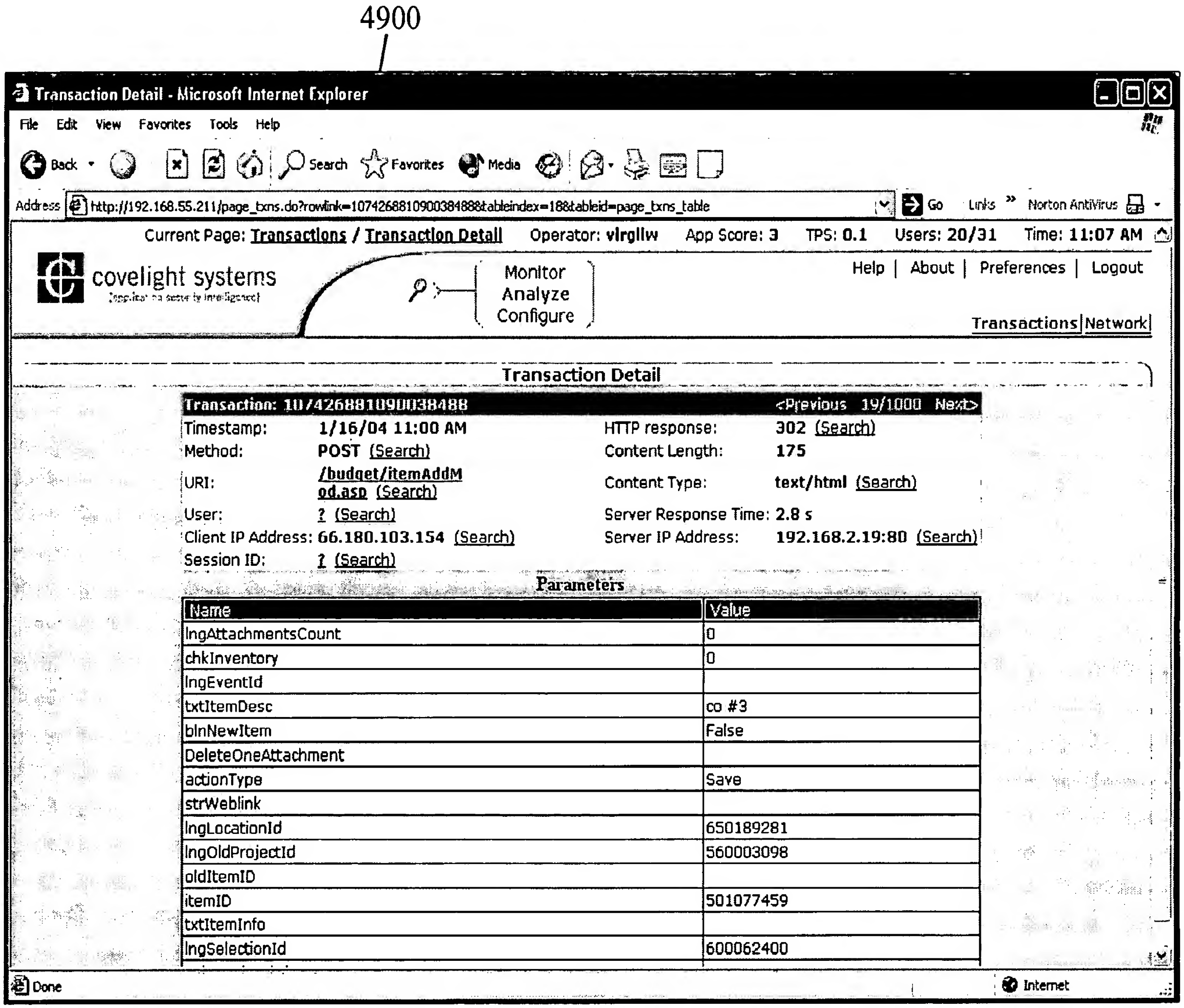
Current Page: Transactions Operator: virgilw App Score: 3 TPS: 0.2 Users: 20/31 Time: 11:00 AM

Transactions

Showing 1-15 of 1000 (29023 Total Items)

Method	URI	User	Status	Content Length	Content Type	Threat Score	Timestamp	Response Time
GET	/	?	302	135	text/html	0	1/16/04 11:00 AM	6
GET	/images/addloc.gif	?	200	1864	image/gif	0	1/16/04 11:00 AM	2
GET	/images/additem.gif	?	200	1529	image/gif	0	1/16/04 11:00 AM	0
GET	/images/selectsum.gif	?	200	2079	image/gif	0	1/16/04 11:00 AM	0
GET	/images/rt_tabnotch.gif	?	200	49	image/gif	0	1/16/04 11:00 AM	0
GET	/images/lt_tabnotch.gif	?	200	48	image/gif	0	1/16/04 11:00 AM	0
GET	/images/s.gif	?	200	43	image/gif	0	1/16/04 11:00 AM	0
GET	/js/menu.js	?	200	897	application/x-javascript	0	1/16/04 11:00 AM	0
GET	/vbs/_utils.vbs	?	200	956	text/vbscript	0	1/16/04 11:00 AM	0
GET	/js/modal.js	?	200	421	application/x-javascript	0	1/16/04 11:00 AM	0
GET	/js/util.js	?	200	5608	application/x-javascript	0	1/16/04 11:00 AM	3
GET	/js/_const.js	?	200	200	application/x-javascript	0	1/16/04 11:00 AM	0
GET	/indude/builder_styles/_stylemain.css	?	200	12924	text/css	0	1/16/04 11:00 AM	0
GET	/budget/itemaddmod.asp	jon	200	5488	text/html	0	1/16/04 11:00 AM	199
GET	/budget/selectionDetail.asp	jon	200	10454	text/html	0	1/16/04 11:00 AM	2026

FIG. 48


4900
Transaction Detail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links » Norton AntiVirus
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Transactions | Network
Done
Internet

http://192.168.55.211/page_txns.do?rowlink=1074268810900384888&tableindex=18&tableid=page_txns_table

Current Page: Transactions / Transaction Detail Operator: virgilw App Score: 3 TPS: 0.1 Users: 20/31 Time: 11:07 AM

Transaction Detail

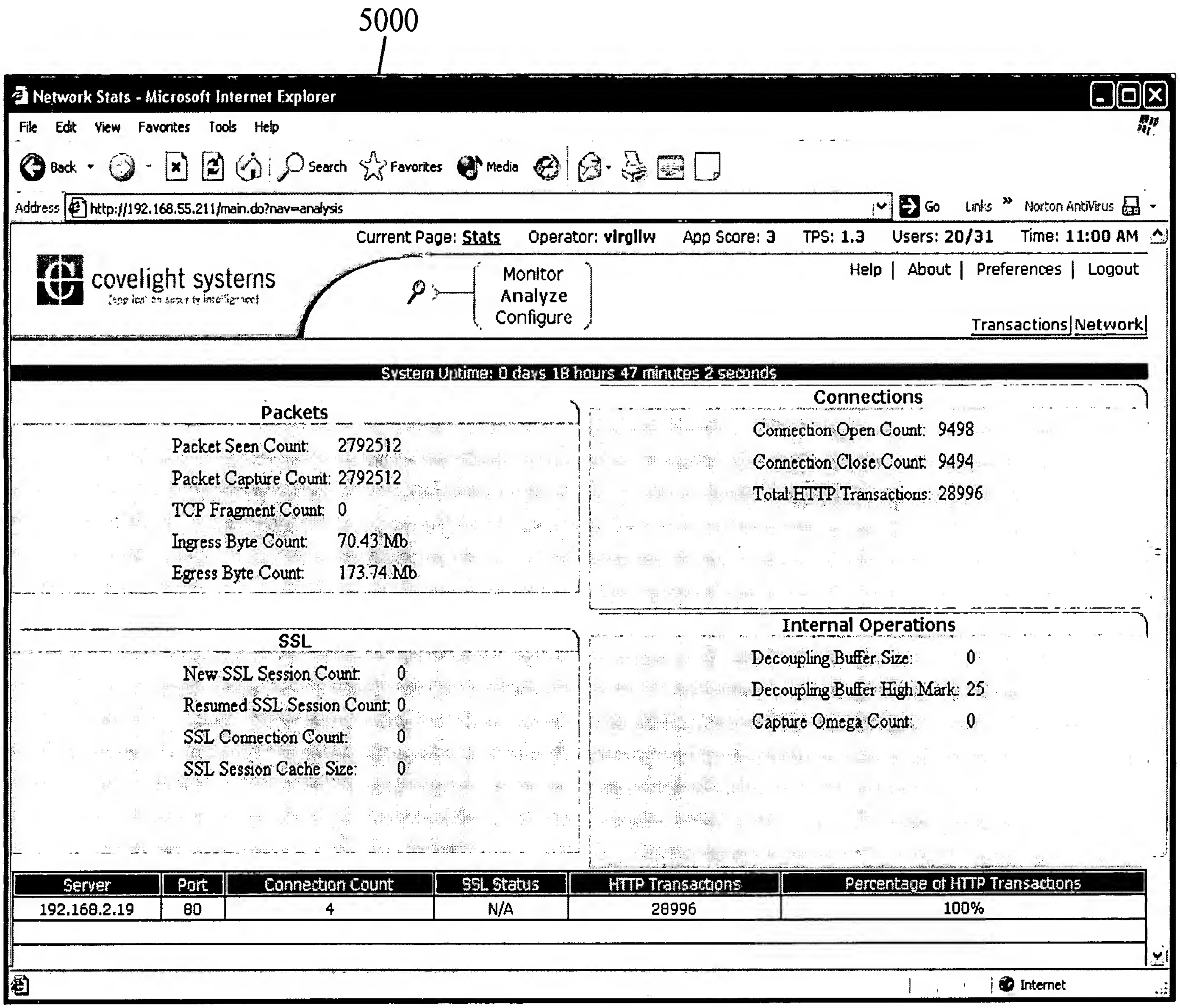
Transaction: 10/4268810900038488 <Previous 19/1000 Next>

Timestamp:	1/16/04 11:00 AM	HTTP response:	302 (Search)
Method:	POST (Search)	Content Length:	175
URI:	/budget/itemAddMod.asp (Search)	Content Type:	text/html (Search)
User:	? (Search)	Server Response Time:	2.8 s
Client IP Address:	66.180.103.154 (Search)	Server IP Address:	192.168.2.19:80 (Search)
Session ID:	? (Search)		

Parameters

Name	Value
lngAttachmentsCount	0
chkInventory	0
lngEventId	
txtItemDesc	co #3
blnNewItem	False
DeleteOneAttachment	
actionType	Save
strWeblink	
lngLocationId	650189281
lngOldProjectId	560003098
oldItemID	
itemID	501077459
txtItemInfo	
lngSelectionId	600062400

FIG. 49



Address: http://192.168.55.211/main.do?nav=analysis

Current Page: Stats Operator: virgilw App Score: 3 TPS: 1.3 Users: 20/31 Time: 11:00 AM

System Uptime: 0 days 18 hours 47 minutes 2 seconds

Packets

Packet Seen Count:	2792512
Packet Capture Count:	2792512
TCP Fragment Count:	0
Ingress Byte Count:	70.43 Mb
Egress Byte Count:	173.74 Mb

Connections

Connection Open Count:	9498
Connection Close Count:	9494
Total HTTP Transactions:	28996

SSL

New SSL Session Count:	0
Resumed SSL Session Count:	0
SSL Connection Count:	0
SSL Session Cache Size:	0

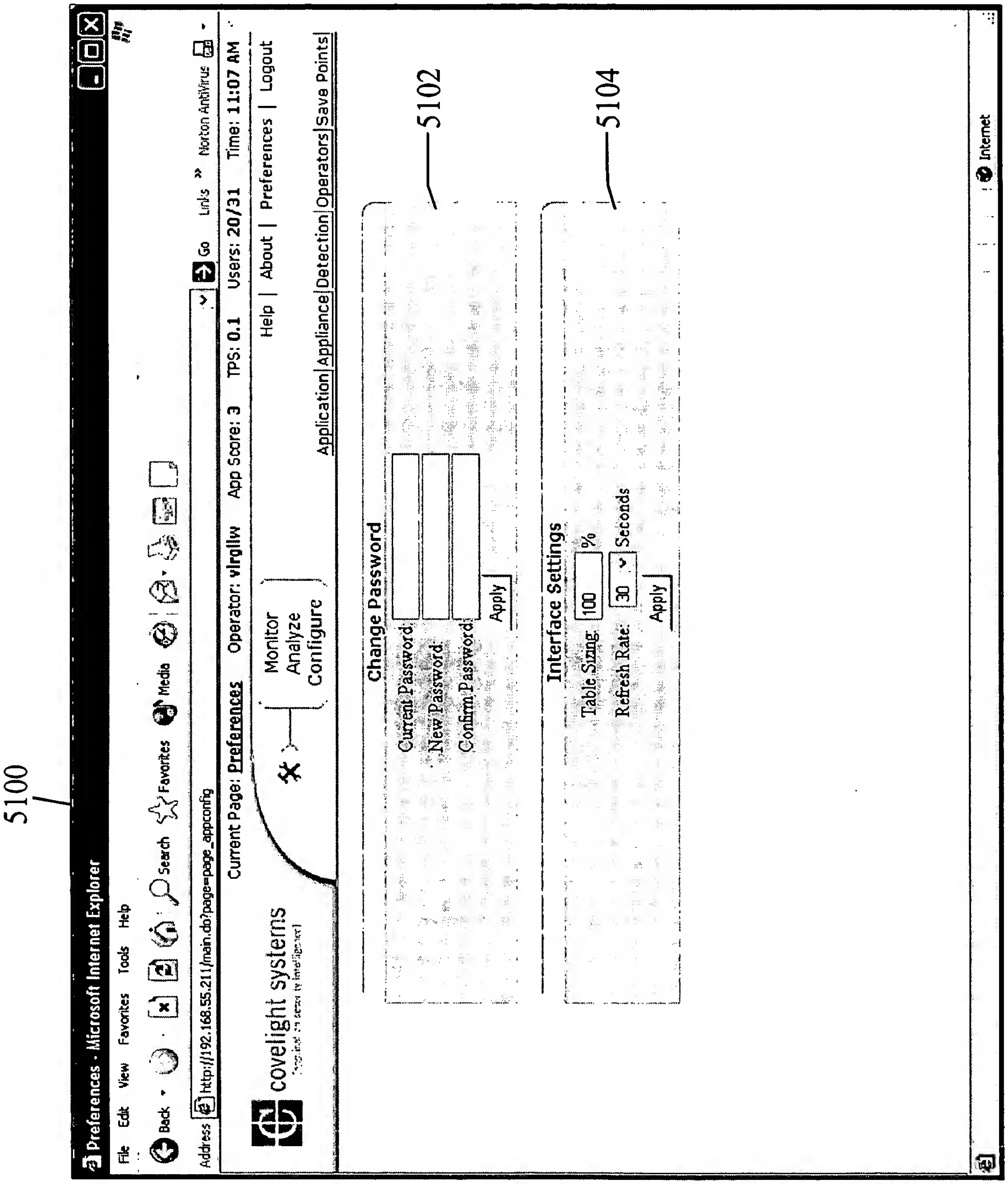
Internal Operations

Decoupling Buffer Size:	0
Decoupling Buffer High Mark:	25
Capture Omega Count:	0

Server	Port	Connection Count	SSL Status	HTTP Transactions	Percentage of HTTP Transactions
192.168.2.19	80	4	N/A	28996	100%

FIG. 50

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6


5100
Preferences - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/main.do?page=page_appconfig
Go Links » Norton AntiVirus
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application Appliance Detection Operators Save Points
5102
5104
Internet

Current Page: Preferences Operator: virgilw App Score: 3 TPS: 0.1 Users: 20/31 Time: 11:07 AM

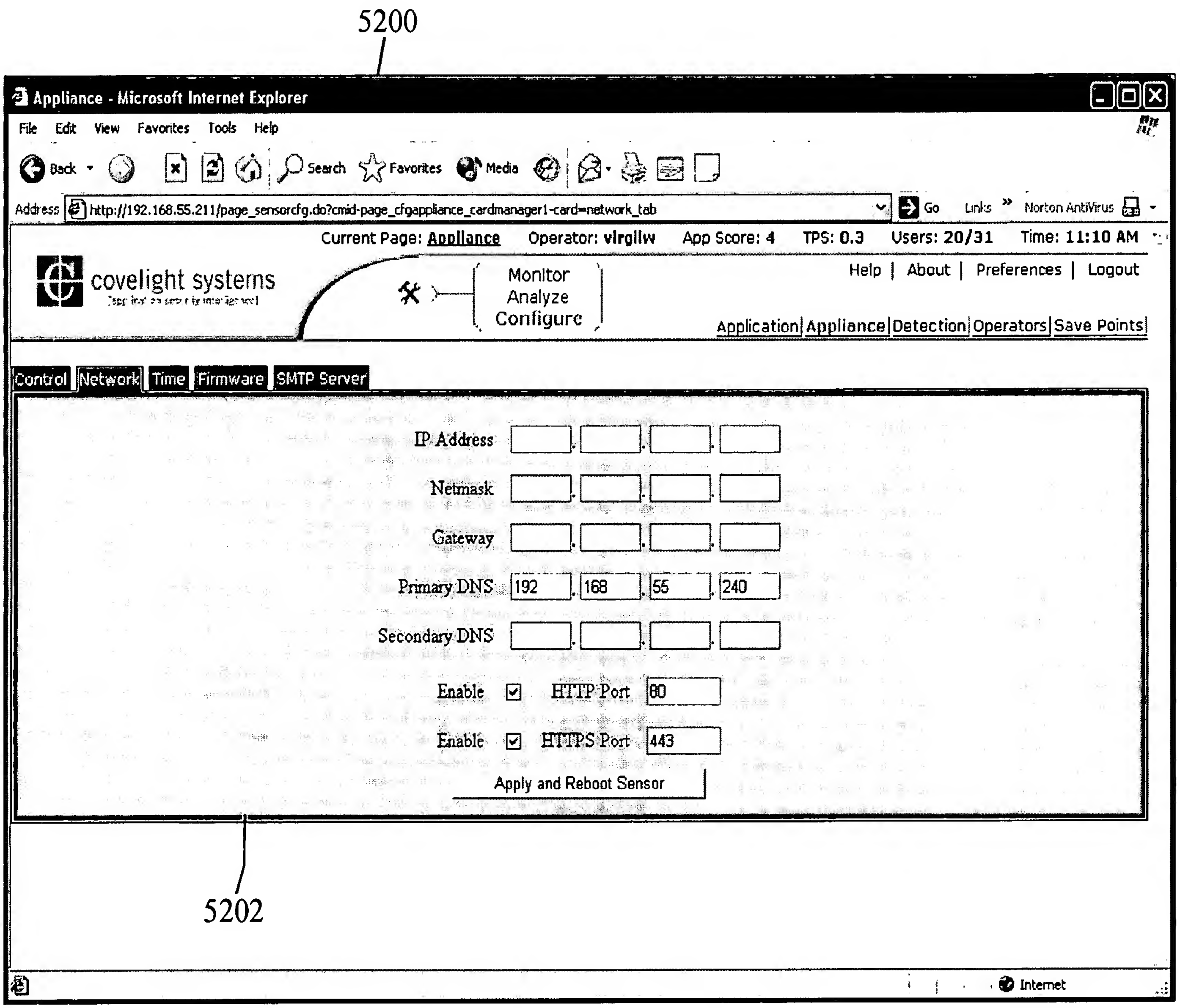
Change Password

Current Password:
New Password:
Confirm Password:
Apply

Interface Settings

Table Sizing: 100 %
Refresh Rate: 30 Seconds
Apply

FIG. 51


5200
Appliance - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links » Norton AntiVirus
covelight systems
Help | About | Preferences | Logout
Monitor
Analyze
Configure
Application | Appliance | Detection | Operators | Save Points
Control Network Time Firmware SMTP Server
Apply and Reboot Sensor
Internet
5202

http://192.168.55.211/page_sensorcfg.do?cmid-page_cfgappliance_cardmanager1-card=network_tab

Current Page: Appliance Operator: virgilw App Score: 4 TPS: 0.3 Users: 20/31 Time: 11:10 AM

IP Address [ ].[ ].[ ].[ ]

Netmask [ ].[ ].[ ].[ ]

Gateway [ ].[ ].[ ].[ ]

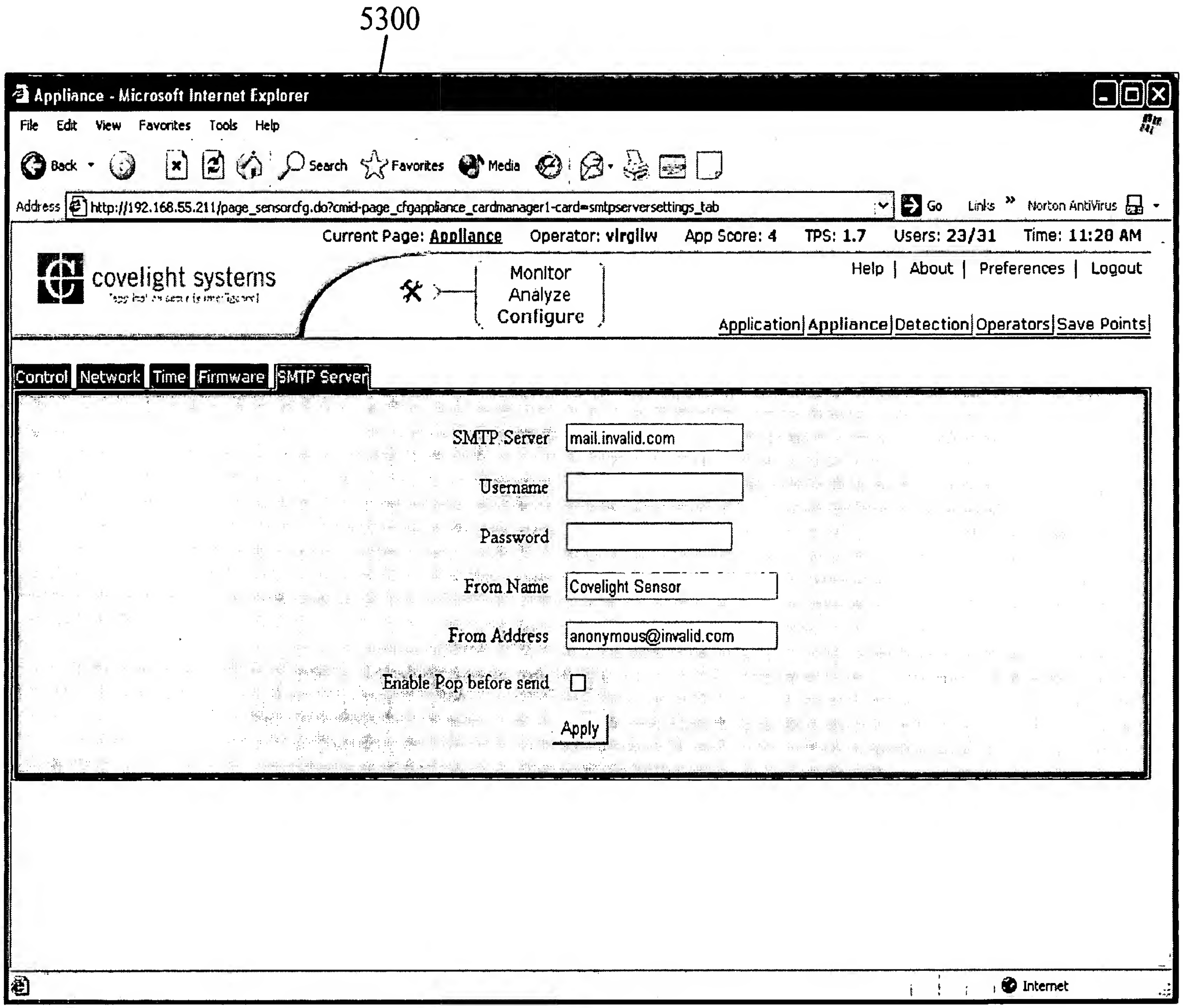
Primary DNS 192.168.55.240

Secondary DNS [ ].[ ].[ ].[ ]

Enable ☑ HTTP Port 80

Enable ☑ HTTPS Port 443

FIG. 52



http://192.168.55.211/page_sensorcfg.do?cmid-page_cfgappliance_cardmanager1-card=smtpserversettings_tab

Current Page: Appliance Operator: virgilw App Score: 4 TPS: 1.7 Users: 23/31 Time: 11:28 AM

SMTP Server: mail.invalid.com

Username:

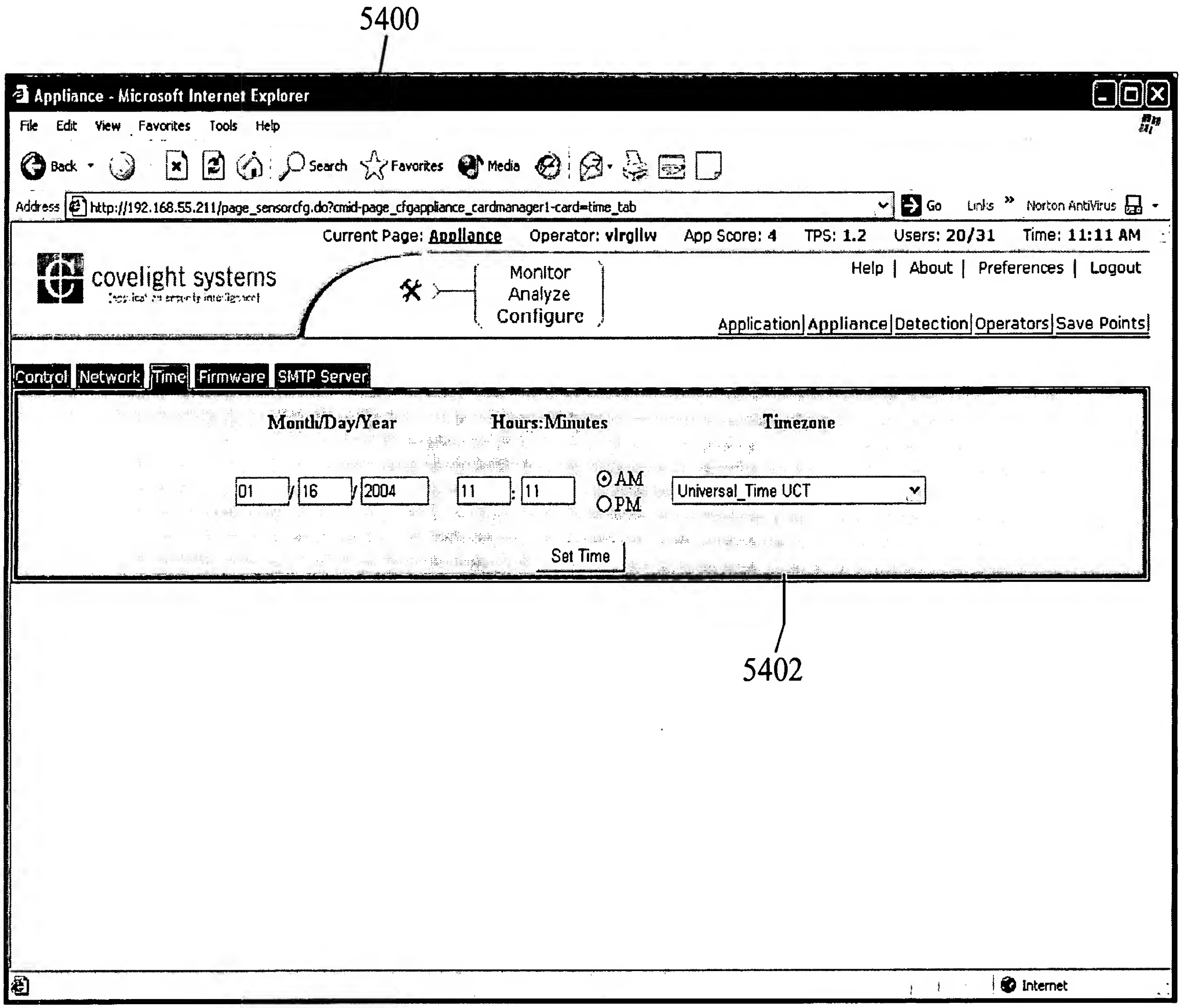
Password:

From Name: Covelight Sensor

From Address: anonymous@invalid.com

Enable Pop before send □

FIG. 53


5400
Appliance - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links » Norton AntiVirus
covelight systems
Help | About | Preferences | Logout
Monitor
Analyze
Configure
Application | Appliance | Detection | Operators | Save Points
Control Network Time Firmware SMTP Server
Set Time
5402
Internet

Address: http://192.168.55.211/page_sensorcfg.do?cmid-page_cfgappliance_cardmanager1-card=time_tab

Current Page: Appliance Operator: vlrgllw App Score: 4 TPS: 1.2 Users: 20/31 Time: 11:11 AM

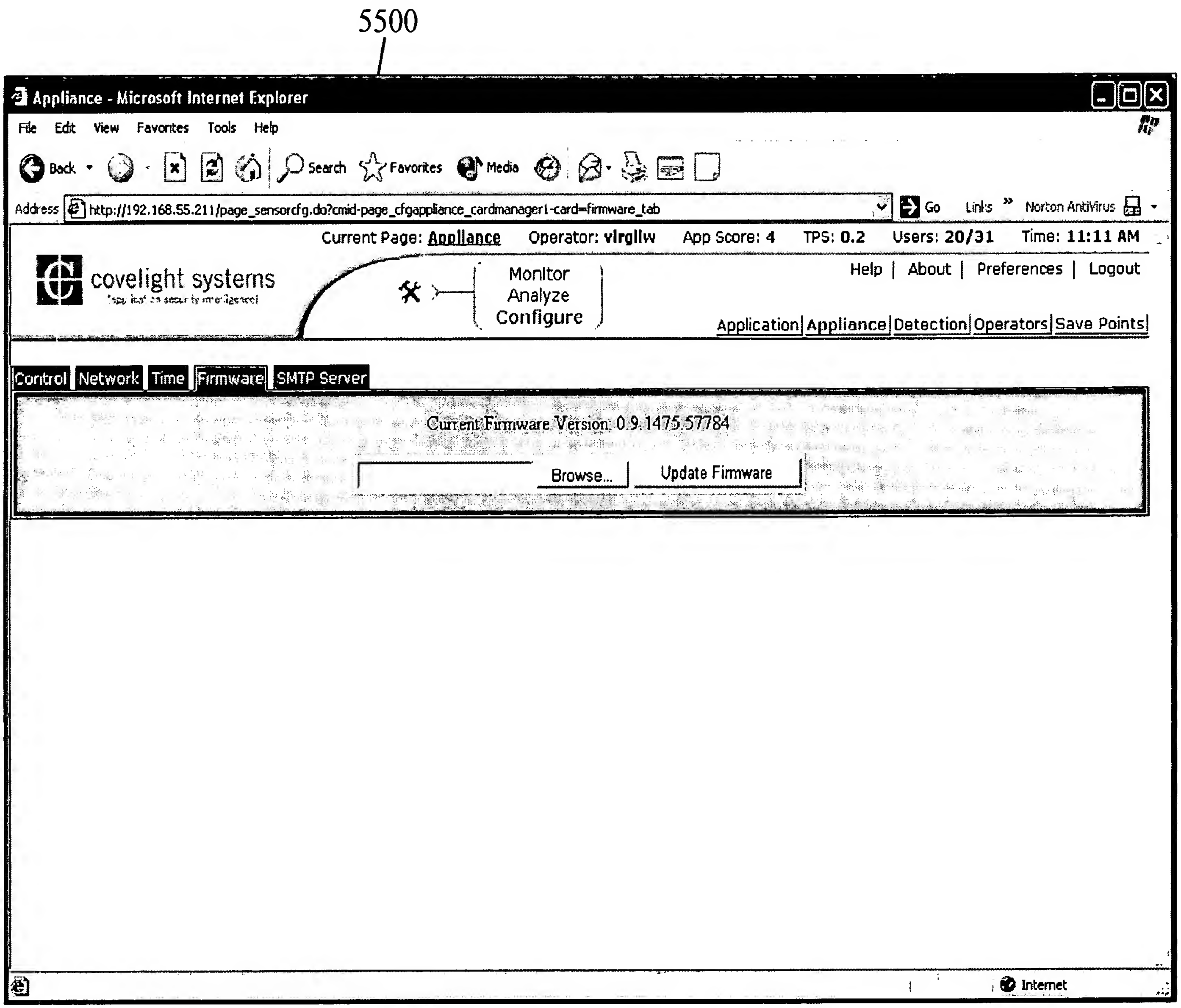
Month/Day/Year: 01 / 16 / 2004

Hours:Minutes: 11 : 11 ● AM ○ PM

Timezone: Universal_Time UCT

FIG. 54

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6



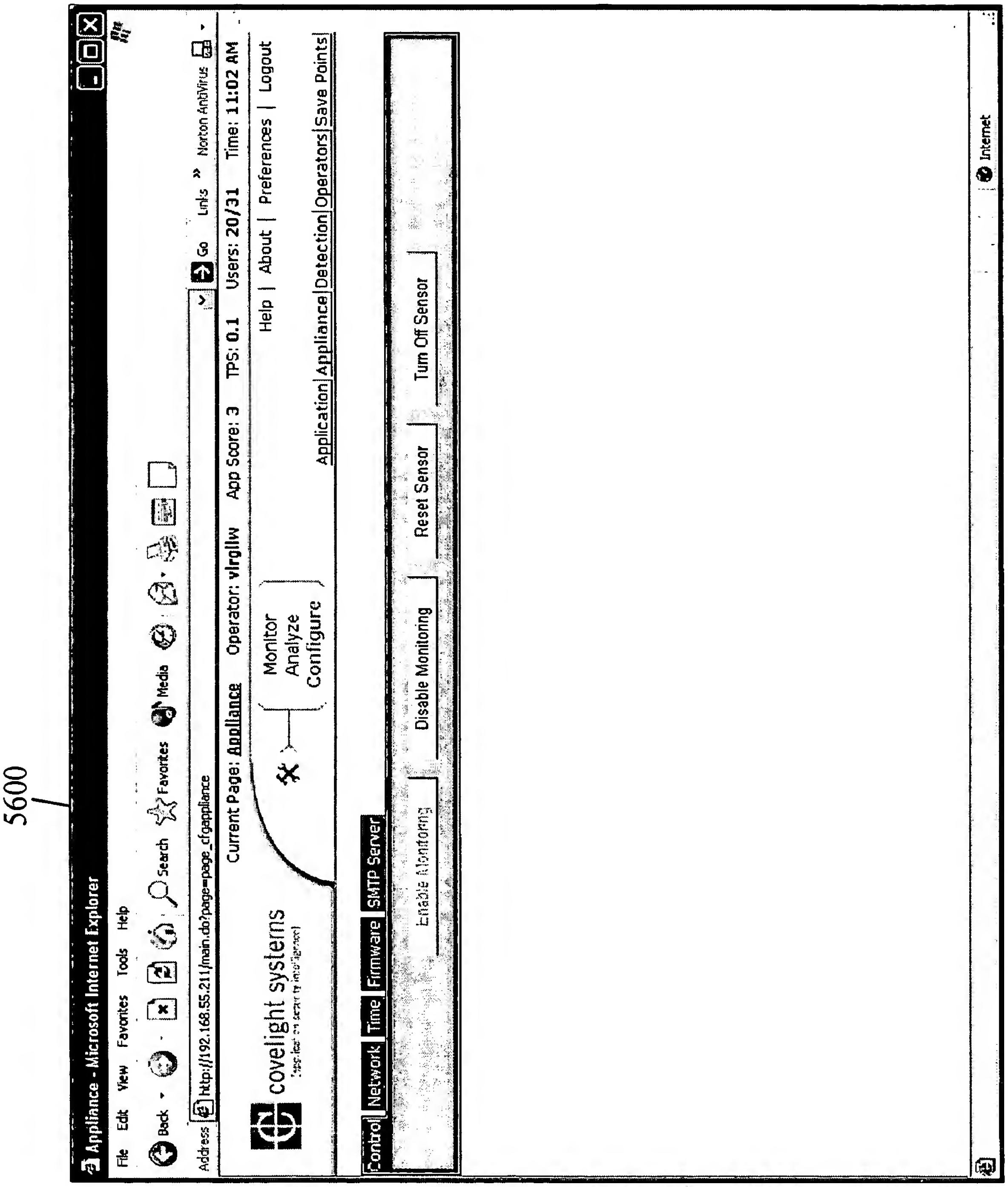
http://192.168.55.211/page_sensorcfg.do?cmid-page_cfgappliance_cardmanager1-card=firmware_tab

Current Page: Appliance Operator: virgilw App Score: 4 TPS: 0.2 Users: 20/31 Time: 11:11 AM

Current Firmware Version: 0.9.1475.57784

FIG. 55

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

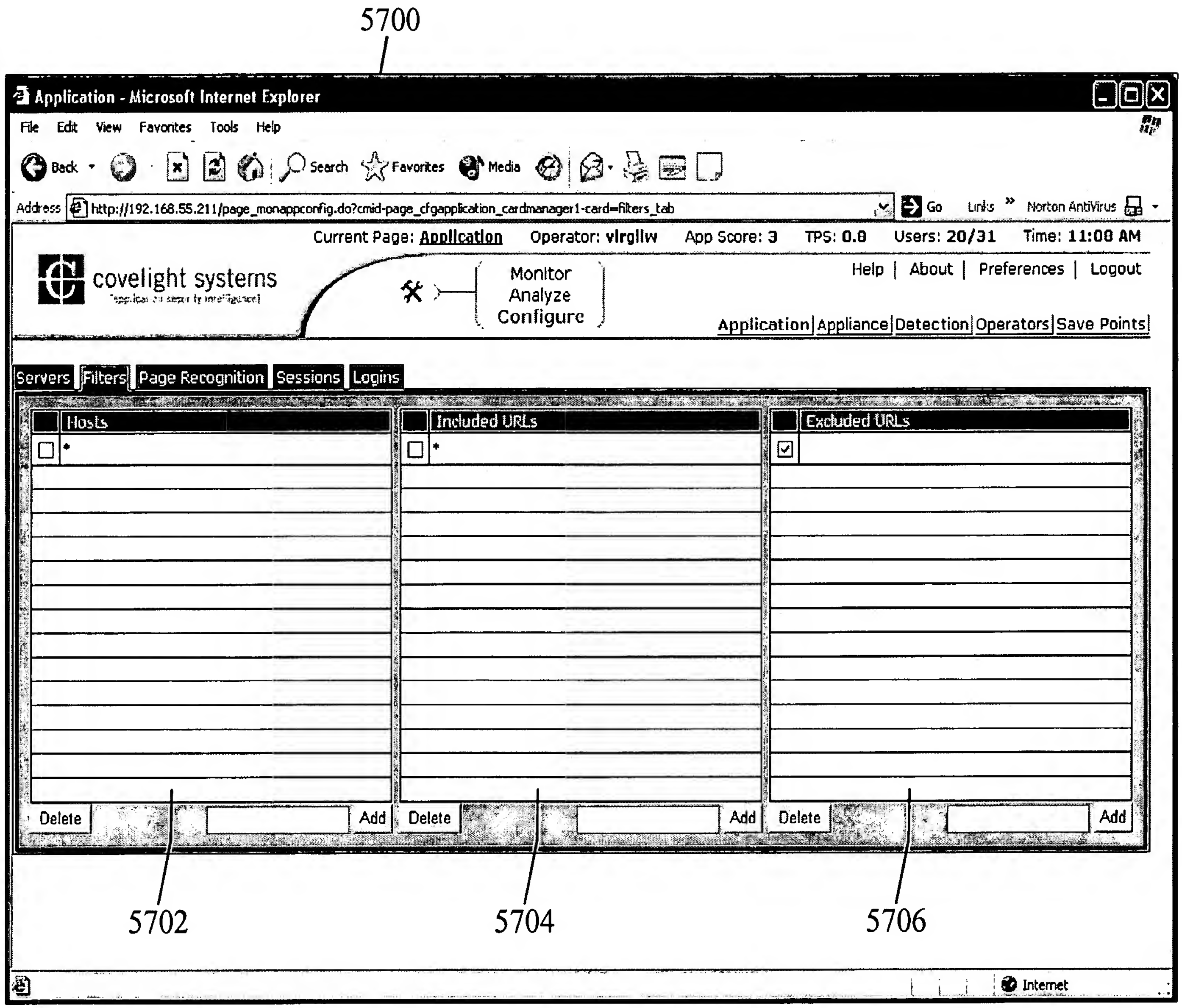

5600
Appliance - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Links
Norton AntiVirus
covelight systems
Help | About | Preferences | Logout
Monitor
Analyze
Configure
Application | Appliance | Detection | Operators | Save Points
Control | Network | Time | Firmware | SMTP Server
Enable Monitoring
Disable Monitoring
Reset Sensor
Turn Off Sensor
Internet

http://192.168.55.211/main.do?page=page_cfgappliance

Current Page: Appliance Operator: virgilw App Score: 3 TPS: 0.1 Users: 20/31 Time: 11:02 AM

FIG. 56

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER
PROGRAM PRODUCTS FOR MONITORING A
SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6



Address http://192.168.55.211/page_monappconfig.do?cmid-page_cfgapplication_cardmanager1-card=filters_tab

Current Page: Application   Operator: virgilw   App Score: 3   TPS: 0.0   Users: 20/31   Time: 11:00 AM

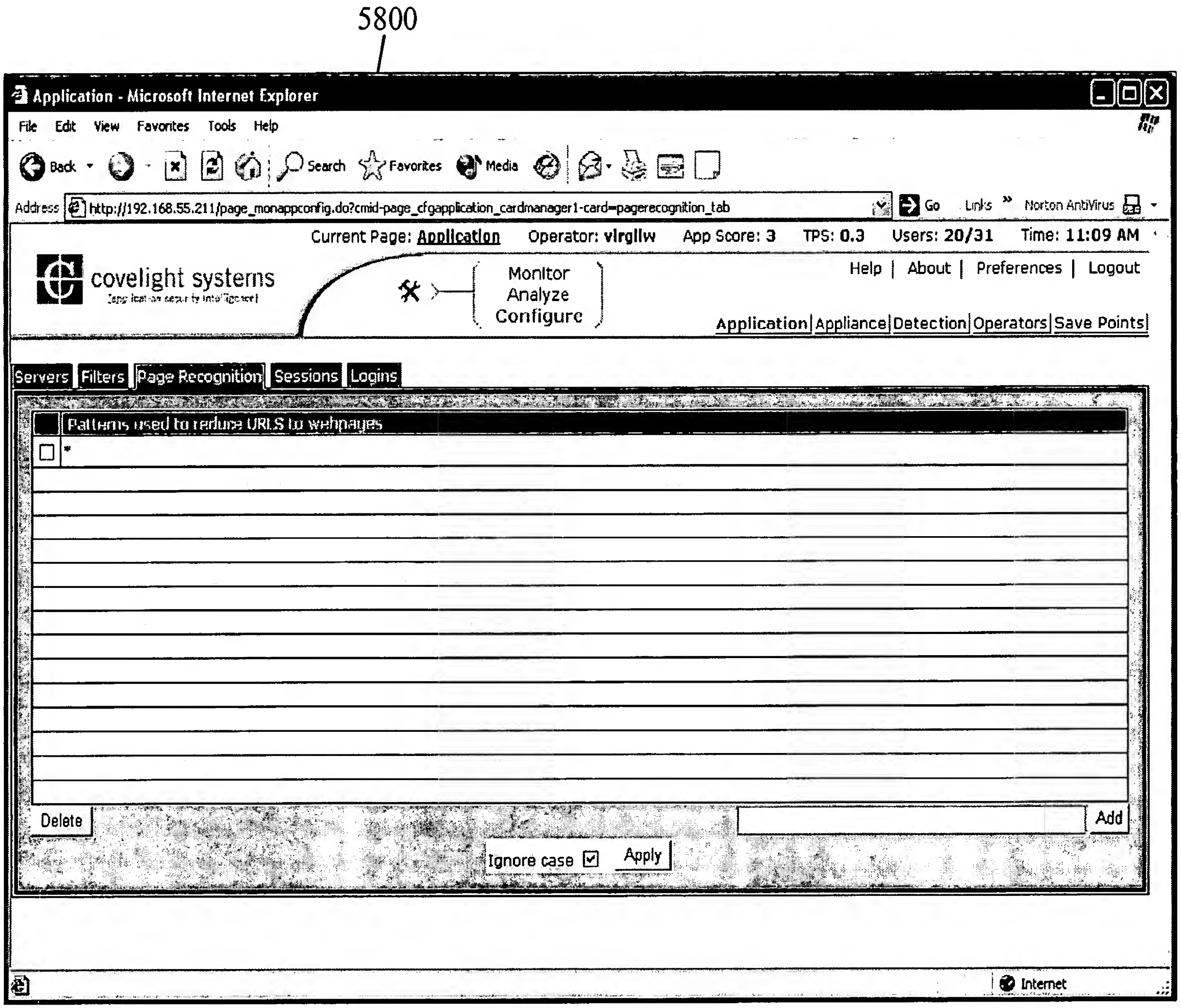
	Hosts
□	*

	Included URLs
□	*

	Excluded URLs
☑	

FIG. 57

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6



http://192.168.55.211/page_monappconfig.do?cmid-page_cfgapplication_cardmanager1-card=pagerecognition_tab

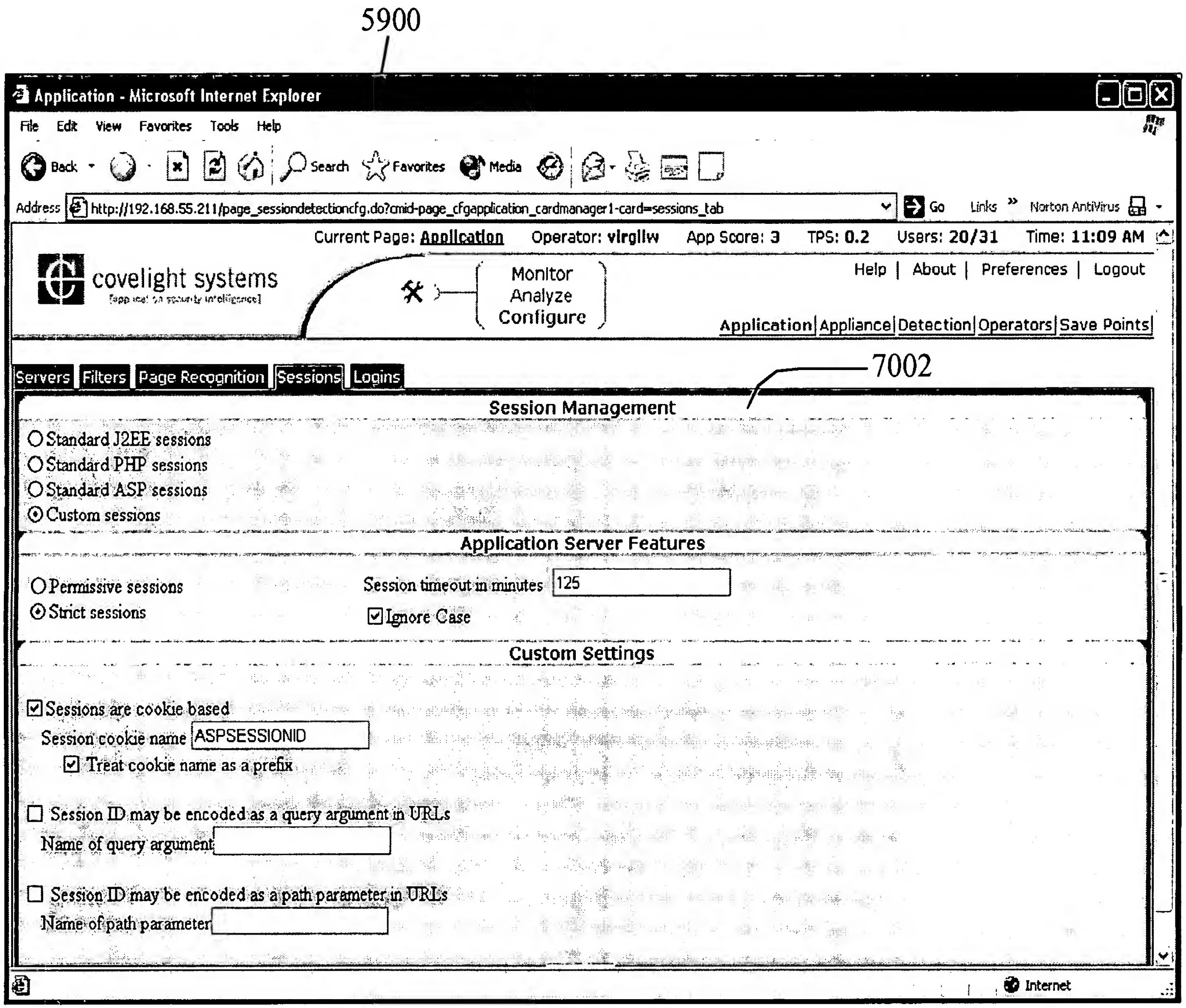
Current Page: Application Operator: virgilw App Score: 3 TPS: 0.3 Users: 20/31 Time: 11:09 AM

	Patterns used to reduce URLS to webpages
□	*

Ignore case ☑

FIG. 58

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6


5900
Application - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_sessiondetectioncfg.do?cmid-page_cfgapplication_cardmanager1-card=sessions_tab
Go Links » Norton AntiVirus
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application | Appliance | Detection | Operators | Save Points
Servers Filters Page Recognition Sessions Logins
7002
Internet

Current Page: Application Operator: virgilw App Score: 3 TPS: 0.2 Users: 20/31 Time: 11:09 AM

Session Management

○ Standard J2EE sessions
○ Standard PHP sessions
○ Standard ASP sessions
● Custom sessions

Application Server Features

○ Permissive sessions
● Strict sessions

Session timeout in minutes: 125
☑ Ignore Case

Custom Settings

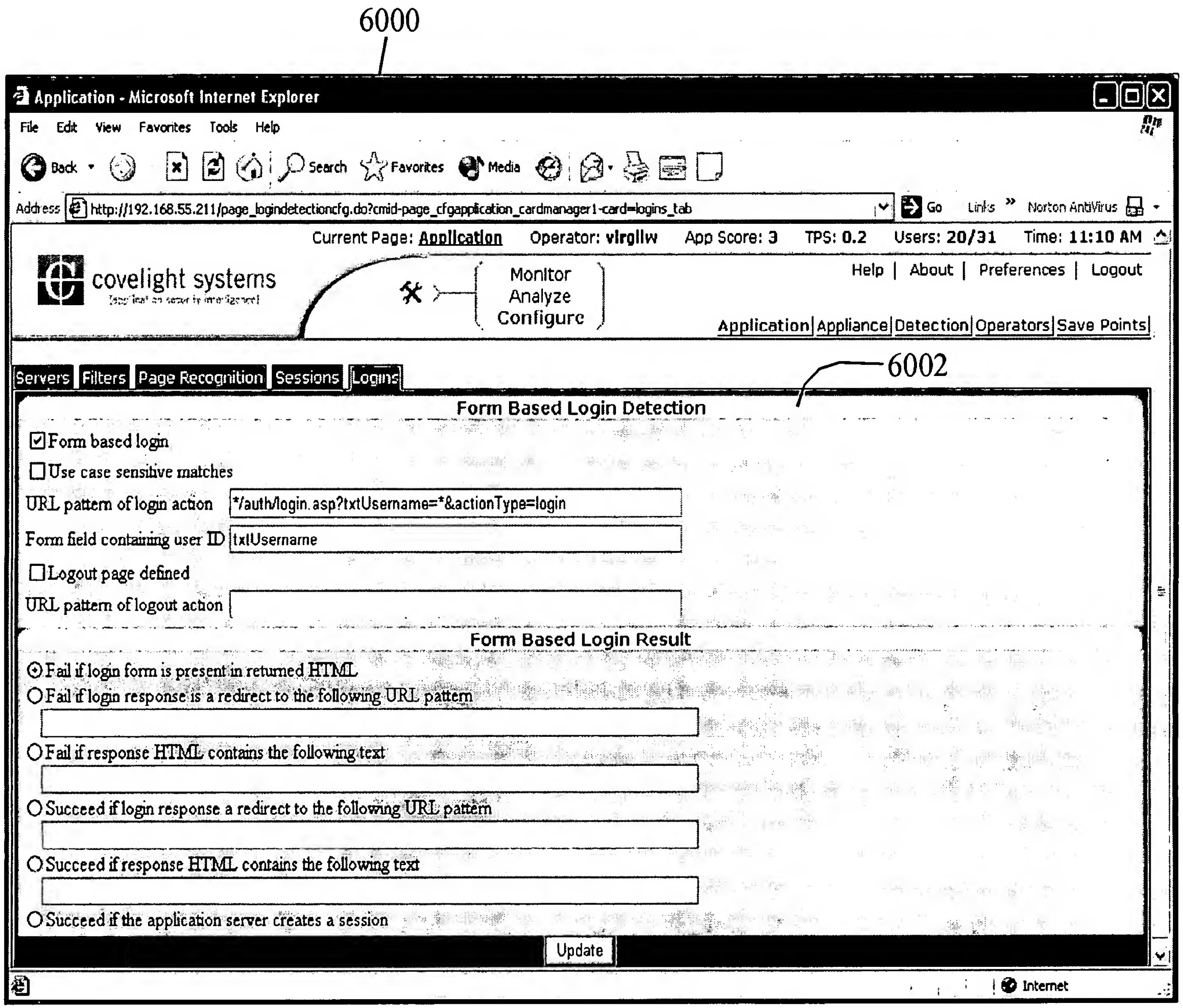
☑ Sessions are cookie based
Session cookie name: ASPSESSIONID
☑ Treat cookie name as a prefix

☐ Session ID may be encoded as a query argument in URLs
Name of query argument:

☐ Session ID may be encoded as a path parameter in URLs
Name of path parameter:

FIG. 59

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER
PROGRAM PRODUCTS FOR MONITORING A
SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6


6000
Application - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links » Norton AntiVirus
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application | Appliance | Detection | Operators | Save Points
Servers Filters Page Recognition Sessions Logins
6002
Update
Internet

Address: http://192.168.55.211/page_logindetectioncfg.do?cmid-page_cfgapplication_cardmanager1-card=logins_tab

Current Page: Application Operator: virgilw App Score: 3 TPS: 0.2 Users: 20/31 Time: 11:10 AM

Form Based Login Detection

☑ Form based login

□ Use case sensitive matches

URL pattern of login action: */auth/login.asp?txtUsername=*&actionType=login

Form field containing user ID: txtUsername

□ Logout page defined

URL pattern of logout action:

Form Based Login Result

● Fail if login form is present in returned HTML

○ Fail if login response is a redirect to the following URL pattern

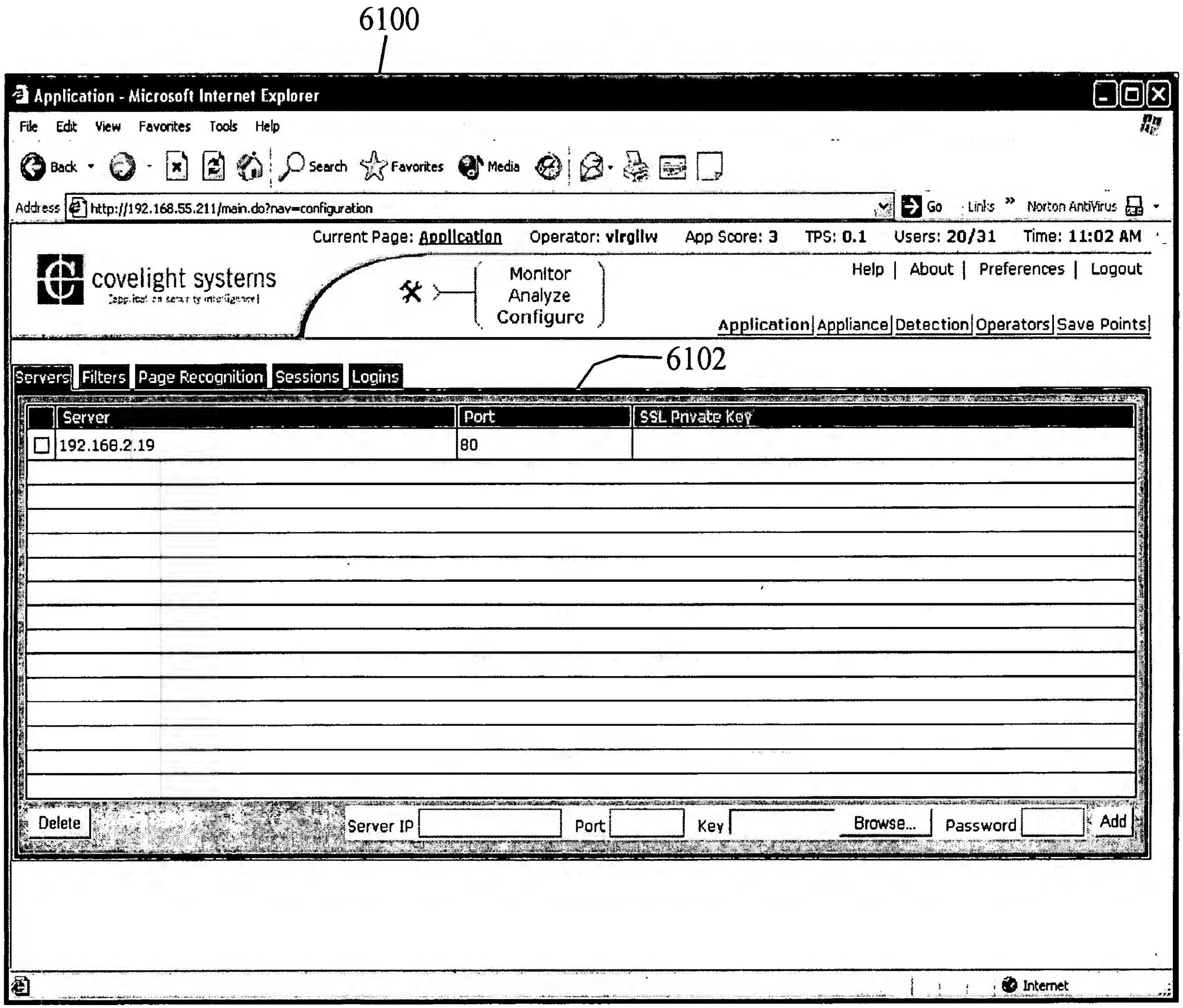
○ Fail if response HTML contains the following text

○ Succeed if login response a redirect to the following URL pattern

○ Succeed if response HTML contains the following text

○ Succeed if the application server creates a session

FIG. 60


6100
Application - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links Norton AntiVirus
covelight systems
Help | About | Preferences | Logout
Monitor
Analyze
Configure
Application | Appliance | Detection | Operators | Save Points
Servers Filters Page Recognition Sessions Logins
6102
Delete
Browse...
Add
Internet

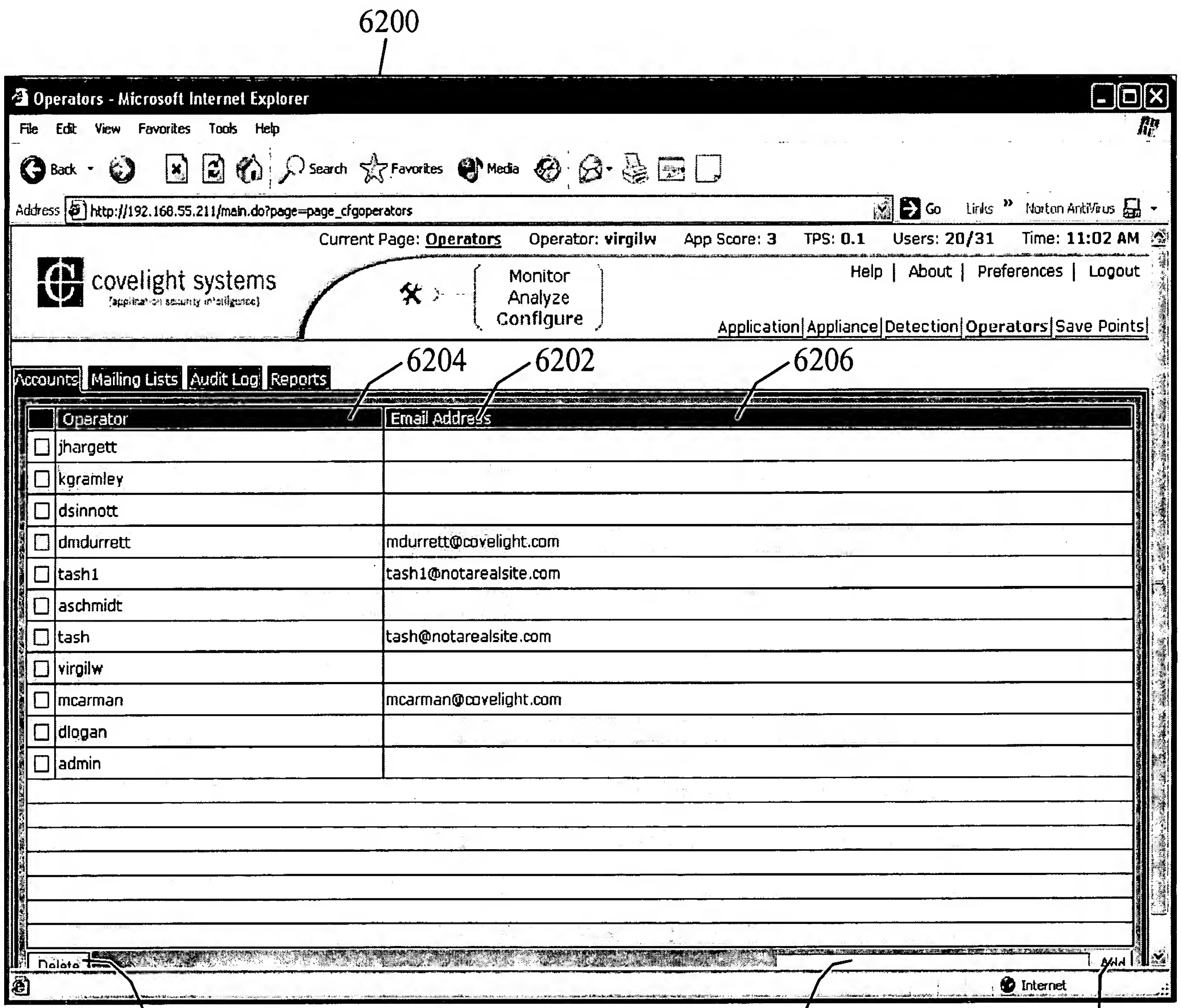
http://192.168.55.211/main.do?nav=configuration

Current Page: Application Operator: virgilw App Score: 3 TPS: 0.1 Users: 20/31 Time: 11:02 AM

	Server	Port	SSL Private Key
□	192.168.2.19	80	

Server IP [ ] Port [ ] Key [ ] Password [ ]

FIG. 61


6200
Operators - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links
Norton AntiVirus
covelight systems
(application security intelligence)
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application | Appliance | Detection | Operators | Save Points
Accounts
Mailing Lists
Audit Log
Reports
6204
6202
6206
Delete
Add
Internet
6208
6212
6210

http://192.168.55.211/main.do?page=page_cfgoperators

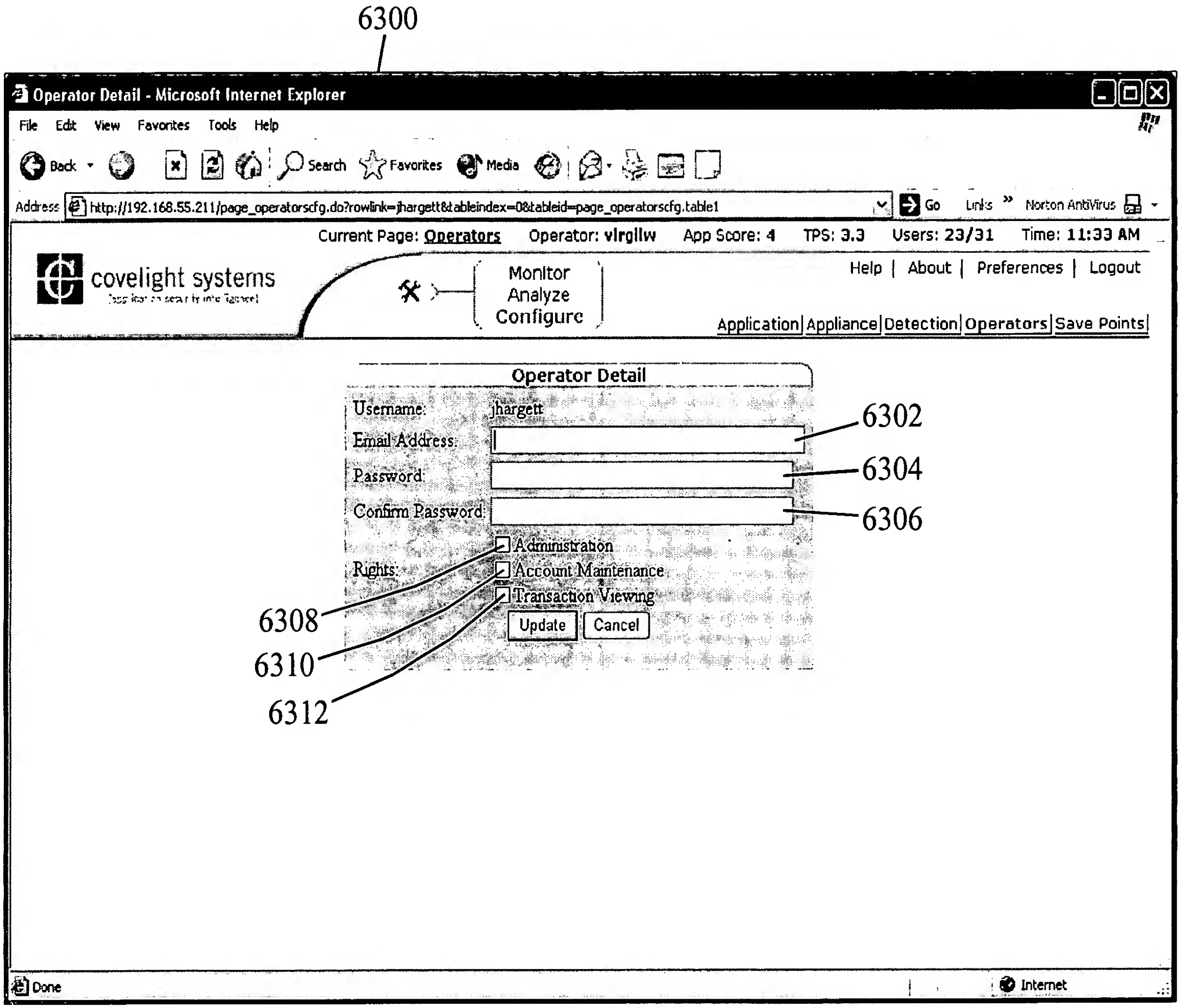
Current Page: Operators Operator: virgilw App Score: 3 TPS: 0.1 Users: 20/31 Time: 11:02 AM

	Operator	Email Address
□	jhargett	
□	kgramley	
□	dsinnott	
□	dmdurrett	mdurrett@covelight.com
□	tash1	tash1@notarealsite.com
□	aschmidt	
□	tash	tash@notarealsite.com
□	virgilw	
□	mcarman	mcarman@covelight.com
□	dlogan	
□	admin	

FIG. 62

REPLACEMENT SHEET

Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6


6300
Operator Detail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links » Norton AntiVirus
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application | Appliance | Detection | Operators | Save Points
Update
Cancel
6302
6304
6306
6308
6310
6312
Done
Internet

Address: http://192.168.55.211/page_operatorscfg.do?rowlink=jhargett&tableindex=0&tableid=page_operatorscfg.table1

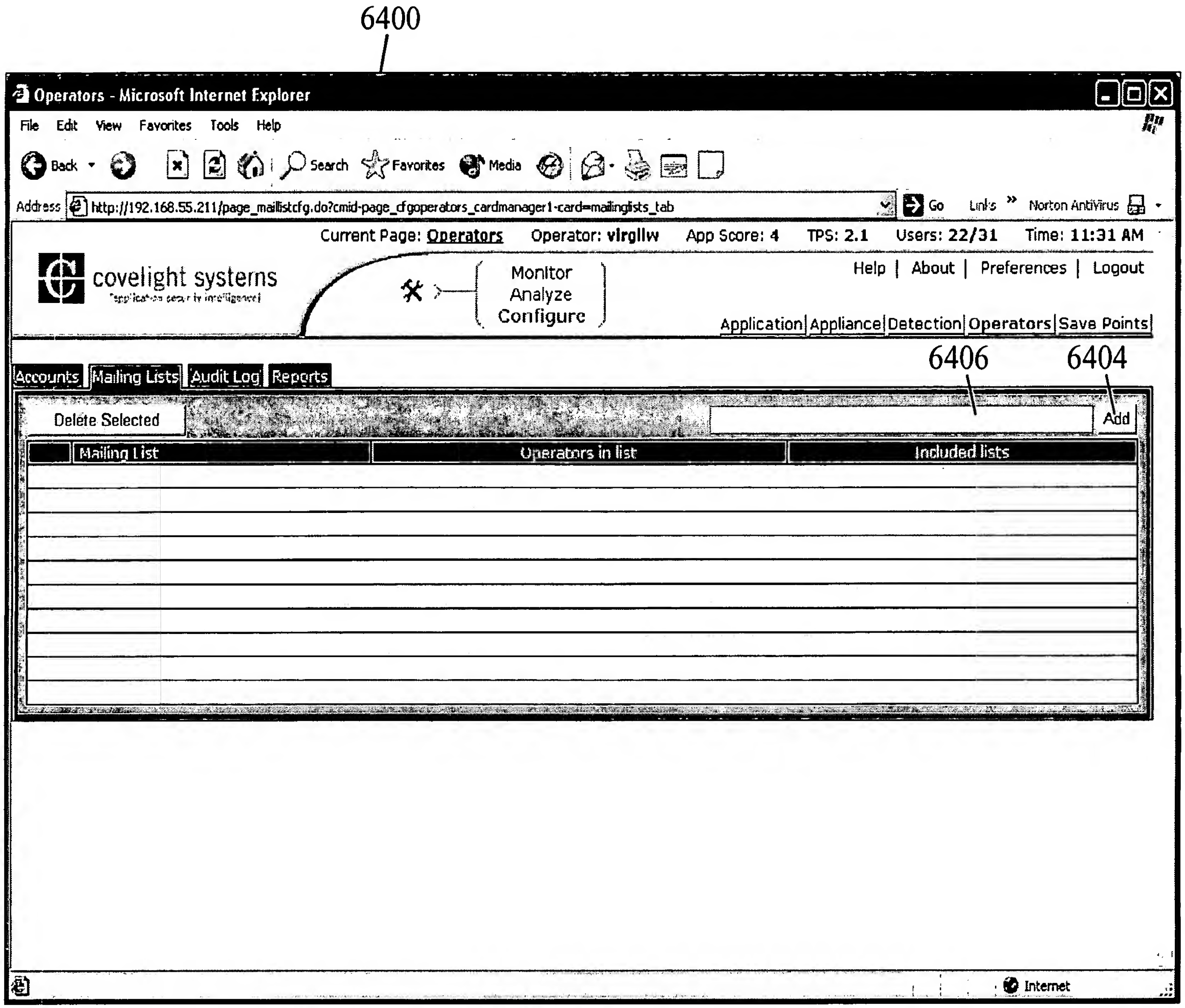
Current Page: Operators Operator: virgilw App Score: 4 TPS: 3.3 Users: 23/31 Time: 11:33 AM

Operator Detail

Username: jhargett
Email Address:
Password:
Confirm Password:
Rights: □ Administration
□ Account Maintenance
□ Transaction Viewing

FIG. 63

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER
PROGRAM PRODUCTS FOR MONITORING A
SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

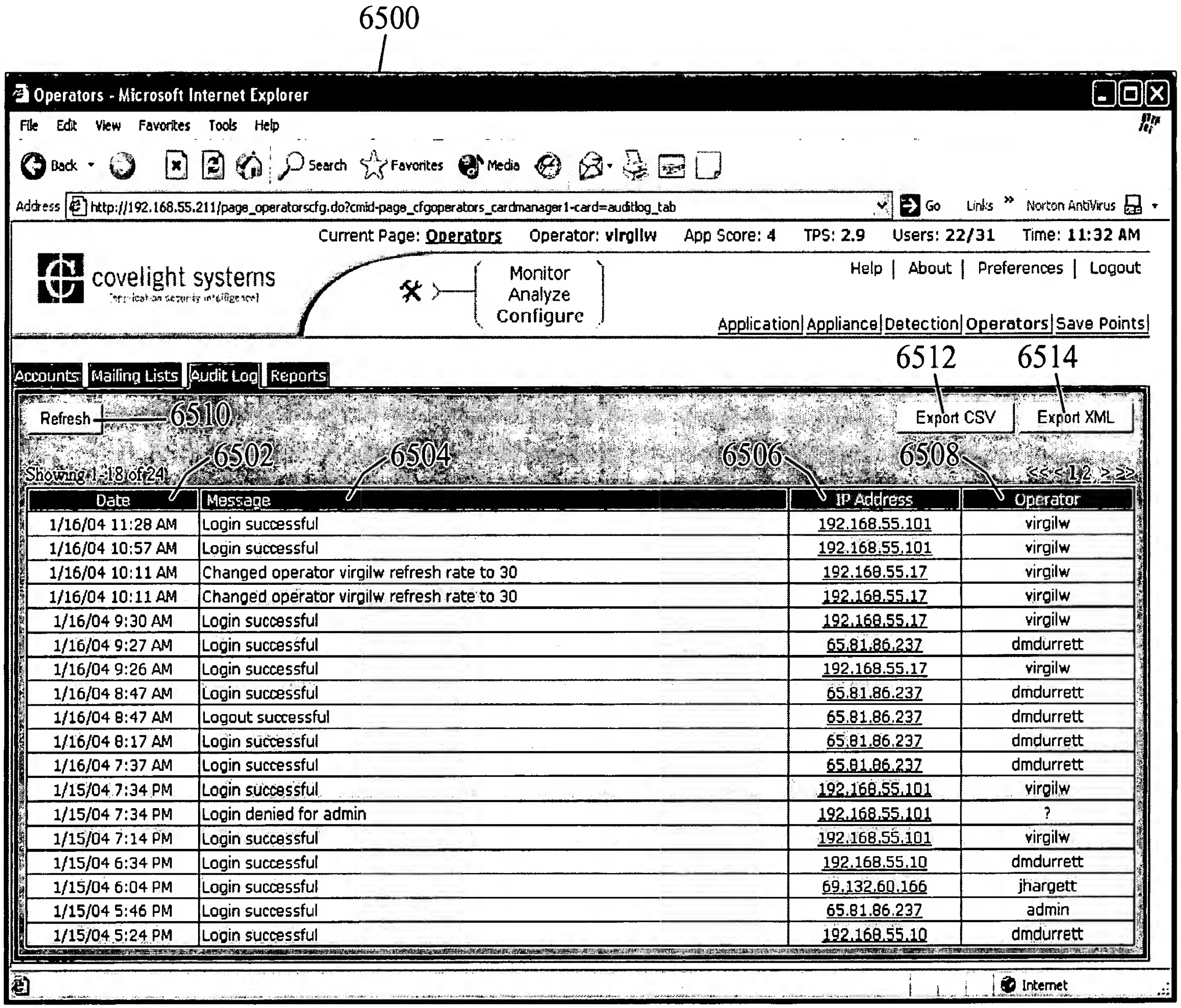

6400
6406
6404
Operators - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Go
Links
Norton AntiVirus
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application | Appliance | Detection | Operators | Save Points
Accounts
Mailing Lists
Audit Log
Reports
Delete Selected
Add
Internet

Address http://192.168.55.211/page_maillistcfg.do?cmid-page_cfgoperators_cardmanager1-card=mailinglists_tab

Current Page: Operators   Operator: virgilw   App Score: 4   TPS: 2.1   Users: 22/31   Time: 11:31 AM

	Mailing List	Operators in list	Included lists

FIG. 64


6500
Operators - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links » Norton AntiVirus
covelight systems
application security intelligence
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application | Appliance | Detection | Operators | Save Points
Accounts Mailing Lists Audit Log Reports
6512
6514
Refresh
6510
Export CSV
Export XML
6502
6504
6506
6508
<< < 1 2 > >>
Internet

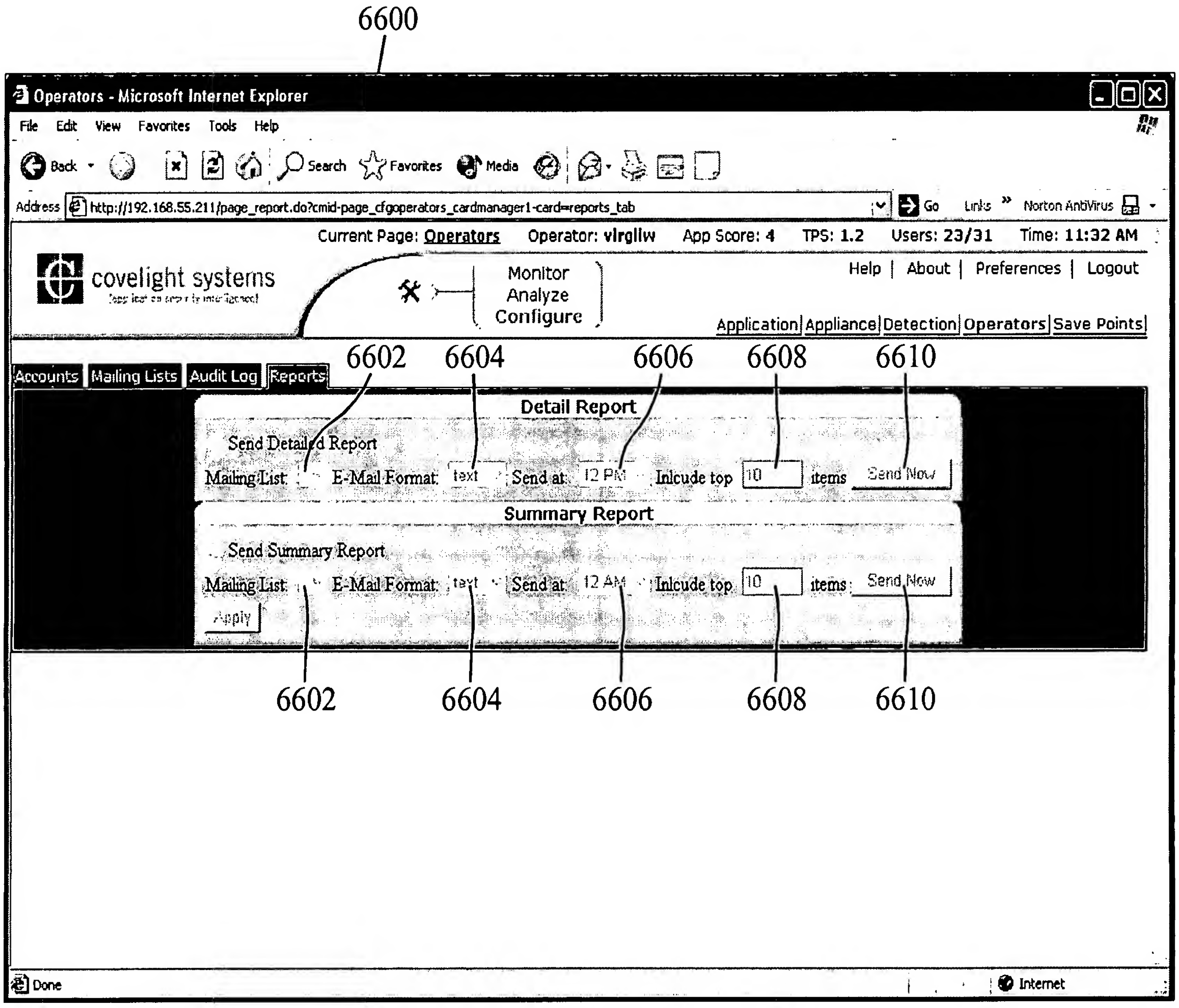
http://192.168.55.211/page_operatorscfg.do?cmid-page_cfgoperators_cardmanager1-card=auditlog_tab

Current Page: Operators Operator: virgilw App Score: 4 TPS: 2.9 Users: 22/31 Time: 11:32 AM

Showing 1-18 of 24

Date	Message	IP Address	Operator
1/16/04 11:28 AM	Login successful	192.168.55.101	virgilw
1/16/04 10:57 AM	Login successful	192.168.55.101	virgilw
1/16/04 10:11 AM	Changed operator virgilw refresh rate to 30	192.168.55.17	virgilw
1/16/04 10:11 AM	Changed operator virgilw refresh rate to 30	192.168.55.17	virgilw
1/16/04 9:30 AM	Login successful	192.168.55.17	virgilw
1/16/04 9:27 AM	Login successful	65.81.86.237	dmdurrett
1/16/04 9:26 AM	Login successful	192.168.55.17	virgilw
1/16/04 8:47 AM	Login successful	65.81.86.237	dmdurrett
1/16/04 8:47 AM	Logout successful	65.81.86.237	dmdurrett
1/16/04 8:17 AM	Login successful	65.81.86.237	dmdurrett
1/16/04 7:37 AM	Login successful	65.81.86.237	dmdurrett
1/15/04 7:34 PM	Login successful	192.168.55.101	virgilw
1/15/04 7:34 PM	Login denied for admin	192.168.55.101	?
1/15/04 7:14 PM	Login successful	192.168.55.101	virgilw
1/15/04 6:34 PM	Login successful	192.168.55.10	dmdurrett
1/15/04 6:04 PM	Login successful	69.132.60.166	jhargett
1/15/04 5:46 PM	Login successful	65.81.86.237	admin
1/15/04 5:24 PM	Login successful	192.168.55.10	dmdurrett

FIG. 65


6600
Operators - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Links » Norton AntiVirus
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application | Appliance | Detection | Operators | Save Points
Accounts
Mailing Lists
Audit Log
Reports
Apply
Done
Internet
6602
6604
6606
6608
6610
6602
6604
6606
6608
6610

http://192.168.55.211/page_report.do?cmid-page_cfgoperators_cardmanager1-card=reports_tab

Current Page: Operators Operator: virgilw App Score: 4 TPS: 1.2 Users: 23/31 Time: 11:32 AM

Detail Report

Send Detailed Report

Mailing List: E-Mail Format: text Send at: 12 PM Inlcude top 10 items Send Now

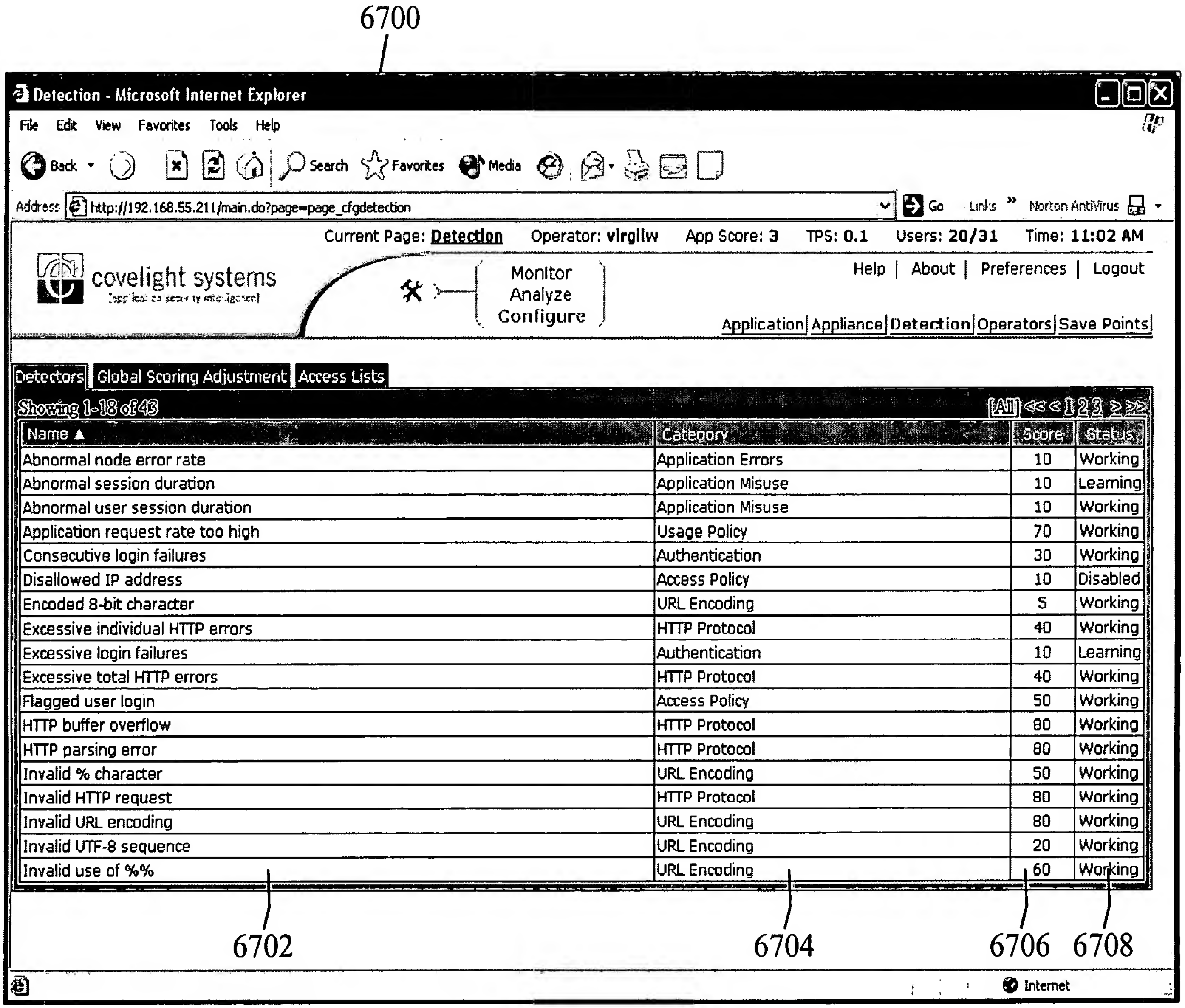
Summary Report

Send Summary Report

Mailing List: E-Mail Format: text Send at: 12 AM Inlcude top 10 items Send Now

FIG. 66

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER
PROGRAM PRODUCTS FOR MONITORING A
SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

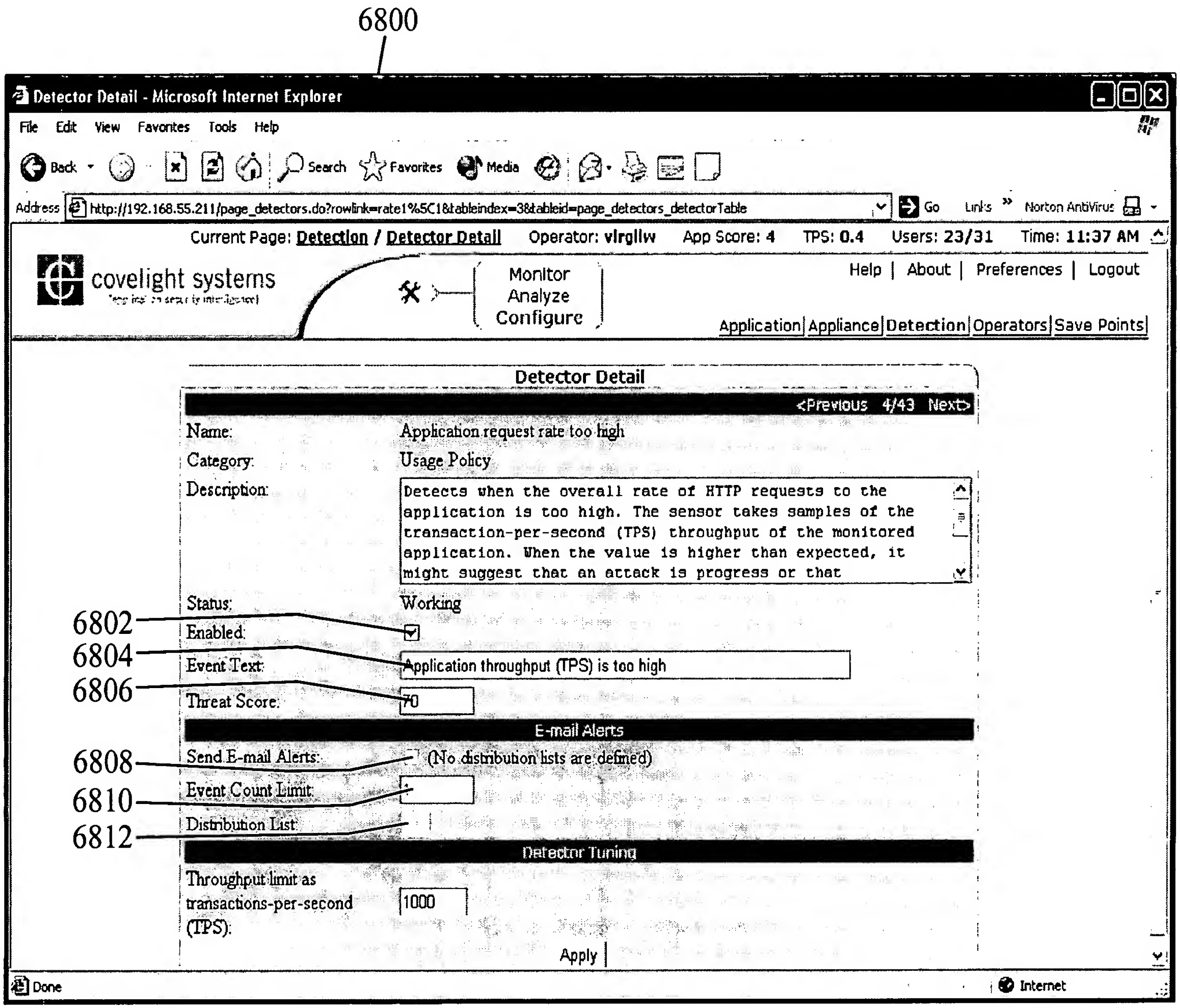

6700
Detection - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address http://192.168.55.211/main.do?page=page_cfgdetection
Go
Links
Norton AntiVirus
covelight systems
application security intelligence
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application Appliance Detection Operators Save Points
Detectors
Global Scoring Adjustment
Access Lists
[All] << < 1 2 3 > >>
6702
6704
6706
6708
Internet

Current Page: Detection Operator: virgilw App Score: 3 TPS: 0.1 Users: 20/31 Time: 11:02 AM

Showing 1-18 of 43

Name ▲	Category	Score	Status
Abnormal node error rate	Application Errors	10	Working
Abnormal session duration	Application Misuse	10	Learning
Abnormal user session duration	Application Misuse	10	Working
Application request rate too high	Usage Policy	70	Working
Consecutive login failures	Authentication	30	Working
Disallowed IP address	Access Policy	10	Disabled
Encoded 8-bit character	URL Encoding	5	Working
Excessive individual HTTP errors	HTTP Protocol	40	Working
Excessive login failures	Authentication	10	Learning
Excessive total HTTP errors	HTTP Protocol	40	Working
Flagged user login	Access Policy	50	Working
HTTP buffer overflow	HTTP Protocol	80	Working
HTTP parsing error	HTTP Protocol	80	Working
Invalid % character	URL Encoding	50	Working
Invalid HTTP request	HTTP Protocol	80	Working
Invalid URL encoding	URL Encoding	80	Working
Invalid UTF-8 sequence	URL Encoding	20	Working
Invalid use of %%	URL Encoding	60	Working

FIG. 67


6800
Detector Detail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links » Norton AntiVirus
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application | Appliance | Detection | Operators | Save Points
<Previous 4/43 Next>
E-mail Alerts
Detector Tuning
Apply
Done
Internet
6802
6804
6806
6808
6810
6812

http://192.168.55.211/page_detectors.do?rowlink=rate1%5C1&tableindex=3&tableid=page_detectors_detectorTable

Current Page: Detection / Detector Detail Operator: virgilw App Score: 4 TPS: 0.4 Users: 23/31 Time: 11:37 AM

Detector Detail

Name: Application request rate too high

Category: Usage Policy

Description: Detects when the overall rate of HTTP requests to the application is too high. The sensor takes samples of the transaction-per-second (TPS) throughput of the monitored application. When the value is higher than expected, it might suggest that an attack is progress or that

Status: Working

Enabled: ☑

Event Text: Application throughput (TPS) is too high

Threat Score: 70

E-mail Alerts

Send E-mail Alerts: (No distribution lists are defined)

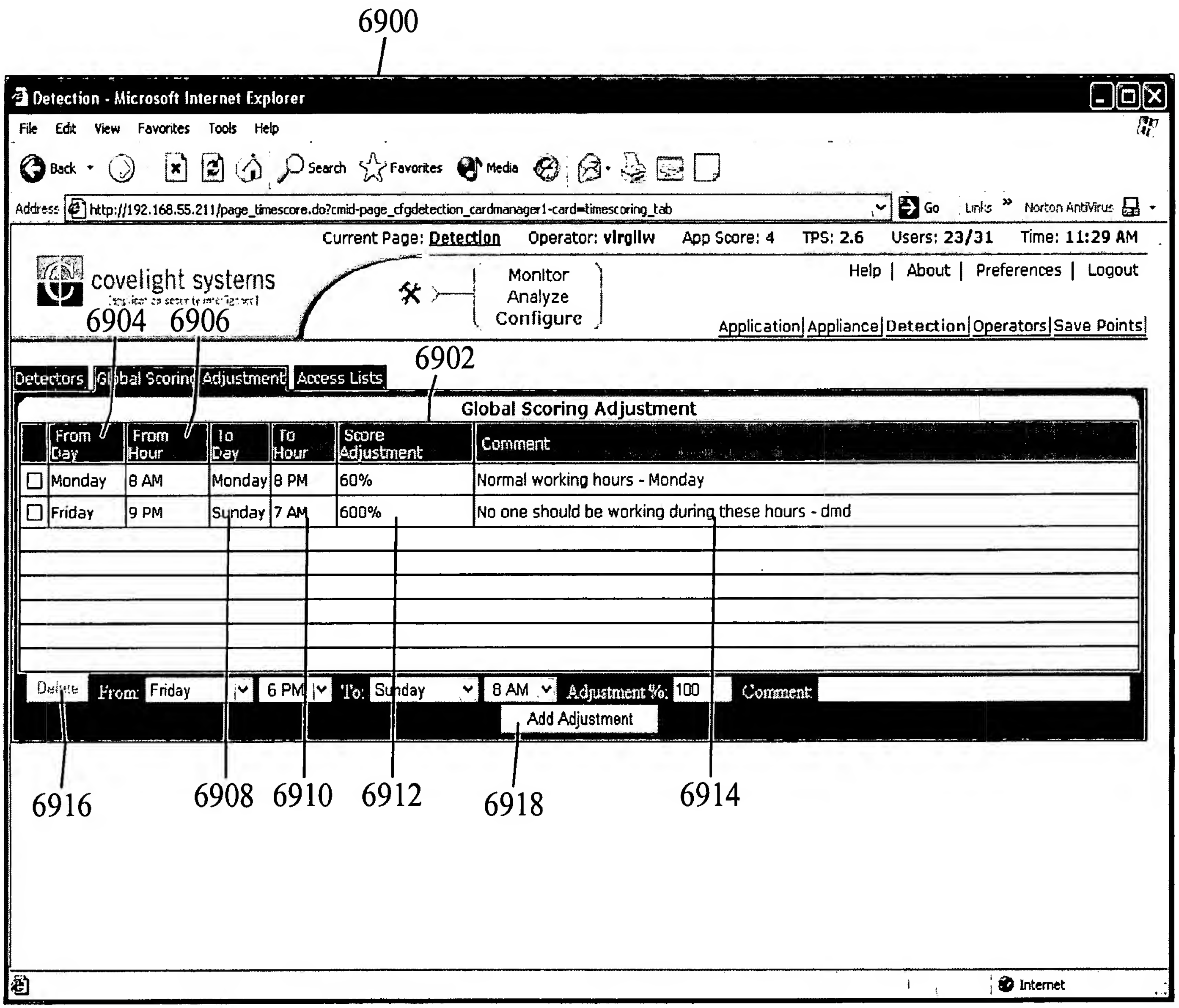
Event Count Limit:

Distribution List:

Detector Tuning

Throughput limit as transactions-per-second (TPS): 1000

FIG. 68


6900
Detection - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_timescore.do?cmid-page_cfgdetection_cardmanager1-card=timescoring_tab
Go Links » Norton AntiVirus
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application Appliance Detection Operators Save Points
Detectors Global Scoring Adjustment Access Lists
6904
6906
6902
Delete
Add Adjustment
6916
6908
6910
6912
6918
6914
Internet

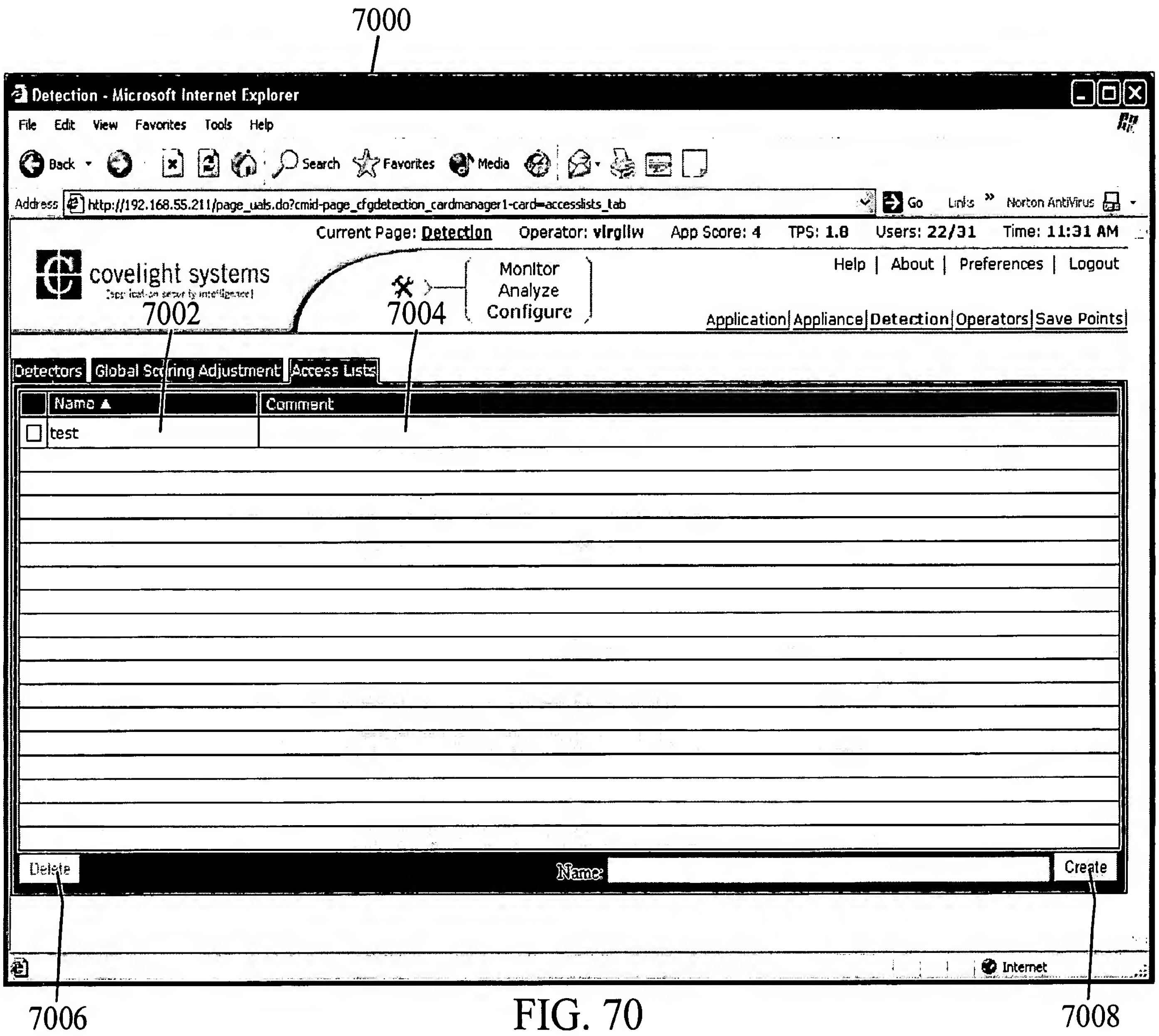
Current Page: Detection Operator: virgilw App Score: 4 TPS: 2.6 Users: 23/31 Time: 11:29 AM

Global Scoring Adjustment

	From Day	From Hour	To Day	To Hour	Score Adjustment	Comment
□	Monday	8 AM	Monday	8 PM	60%	Normal working hours - Monday
□	Friday	9 PM	Sunday	7 AM	600%	No one should be working during these hours - dmd

From: Friday 6 PM To: Sunday 8 AM Adjustment %: 100 Comment:

FIG. 69


7000
Detection - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links » Norton AntiVirus
covelight systems
application security intelligence
7002
7004
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application | Appliance | Detection | Operators | Save Points
Detectors
Global Scoring Adjustment
Access Lists
Delete
Create
Internet
7006
7008

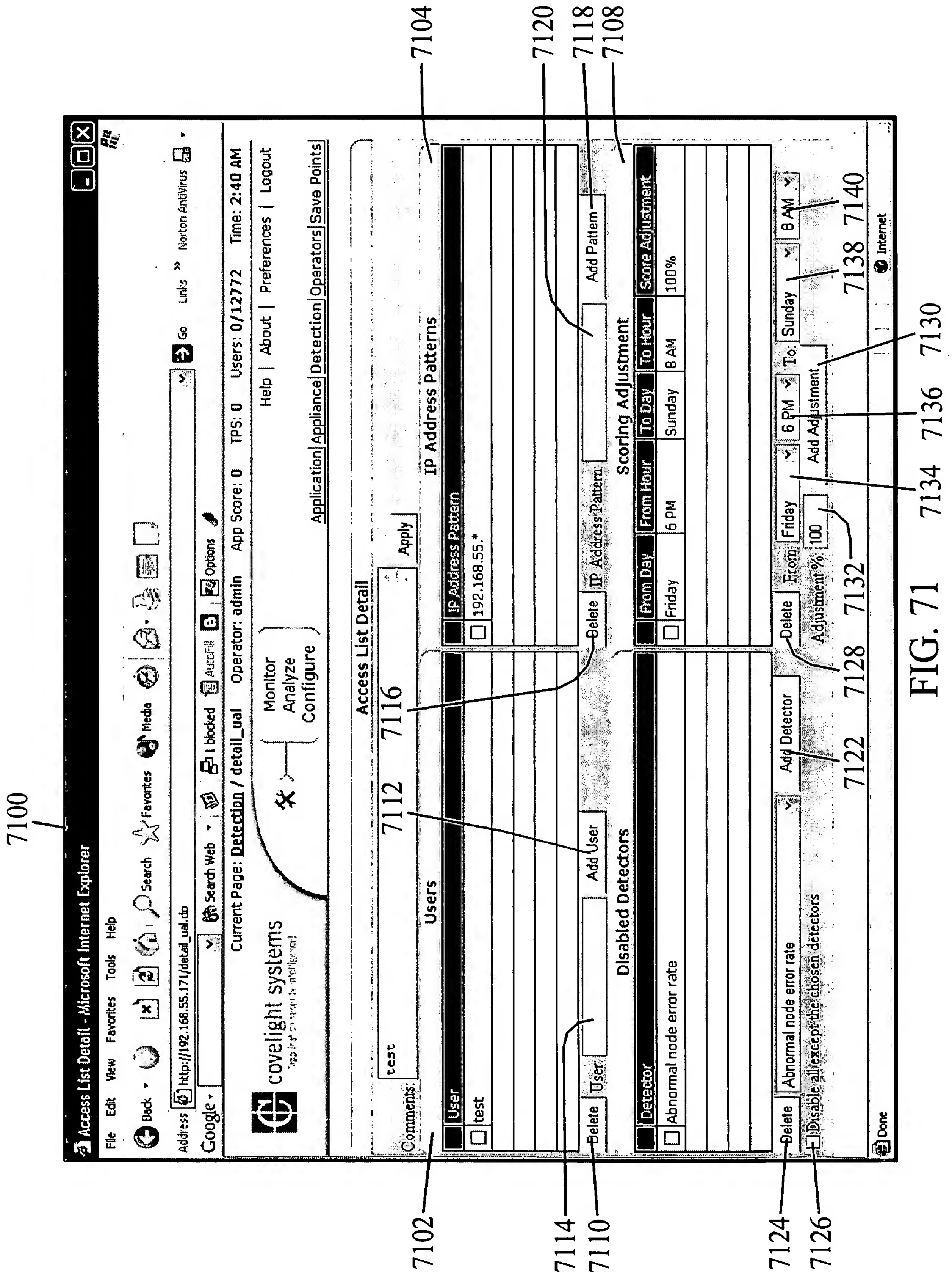
http://192.168.55.211/page_uals.do?cmid-page_cfgdetection_cardmanager1-card=accesslists_tab

Current Page: Detection Operator: virgilw App Score: 4 TPS: 1.8 Users: 22/31 Time: 11:31 AM

	Name ▲	Comment
□	test	

Name:

FIG. 70



Access List Detail - Microsoft Internet Explorer

Address http://192.168.55.171/detail_ual.do

Current Page: Detection / detail_ual Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:40 AM

Help | About | Preferences | Logout

Application | Appliance | Detection | Operators | Save Points

Monitor
Analyze
Configure

Access List Detail

Comments: test Apply

Users

☐	User
☐	test

Delete User Add User

IP Address Patterns

☐	IP Address Pattern
☐	192.168.55.*

Delete IP Address Pattern Add Pattern

Disabled Detectors

☐	Detector
☐	Abnormal node error rate

Delete Abnormal node error rate Add Detector

☐ Disable all except the chosen detectors

Scoring Adjustment

☐	From Day	From Hour	To Day	To Hour	Score Adjustment
☐	Friday	6 PM	Sunday	8 AM	100%

Delete From: Friday 6 PM To: Sunday 8 AM
Adjustment %: 100 Add Adjustment

FIG. 71